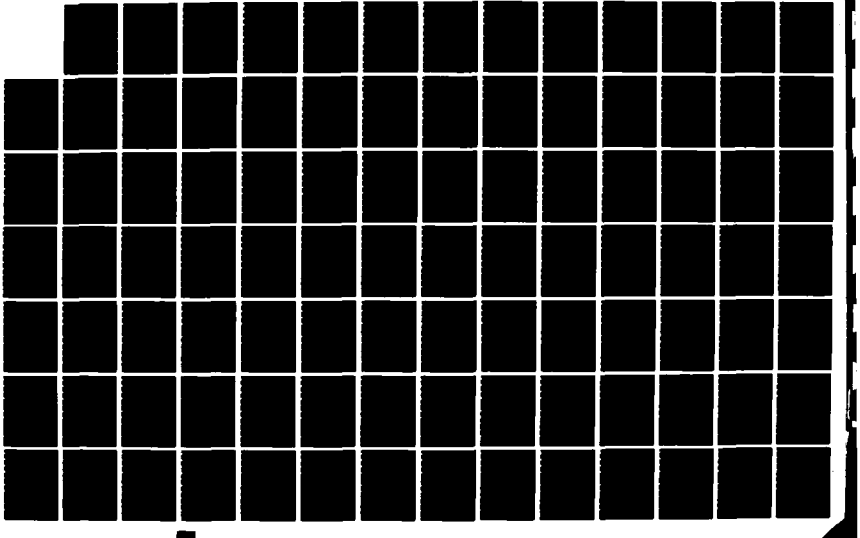
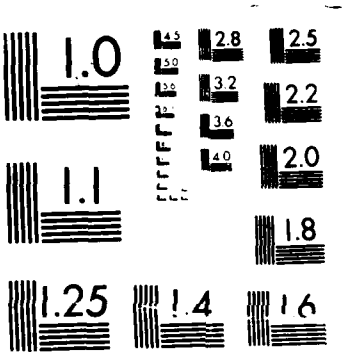
AD-A188 232 ADAPTIVE DESIGN OF A DECISION SUPPORT SYSTEM FOR COMPROMISE ASSESSMENT(U) AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH SCHOOL OF ENGI D T SHIRASAGO 1/2

UNCLASSIFIED MAR 87 AFIT/GST/ENS/87M-16 F/G 12/8 NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS 1963-A

AD-A180 232

DTIC FILE COPY

AFIT/GST/ENS/87M-16

ADAPTIVE DESIGN OF A DECISION SUPPORT SYSTEM FOR COMPROMISE ASSESSMENT

THESIS

Dale T. Shirasago
Captain, USAF

AFIT/GST/ENS/87M-16

MAY 1 5 1987

Approved for public release; distribution unlimited

87 5 15

AFIT/GST/ENS/87M-16

ADAPTIVE DESIGN OF A DECISION SUPPORT SYSTEM FOR COMPROMISE ASSESSMENT

THESIS

Presented to the Faculty of the School of Engineering

of the Air Force Institute of Technology

Air University

In Partial Fulfillment of the

Requirements for the Degree of

Master of Science in Operational Sciences

QUALITY INSPECTED 4

Accession For
NTIS GRA&I
DTIC TAB
Unannounced
Justification
By
Distribution/
Availability Codes
Dist | Avail and/or Special
A-1

Dale T. Shirasago, B.S.

Captain, USAF

March 1987

Approved for public release; distribution unlimited

Table of Contents

		Page
Acknowledgments		iii
List of Figures		iv
List of Tables		v
Abstract		vi
I.	Introduction	1
	Background	2
	Objectives	8
	Scope	10
II.	Historical Development	11
	Related Research	14
	Overview of the DSS Design	17
III.	Methodology	20
	Problem Definition	20
	Kernel Identification	22
	Storyboard	23
	Kernel Development	24
	Hook Book	24
	Evaluation	26
IV.	Resulting System	28
	Computer Systems	28
	Data	29
	System Operation	34
	Additional Functions	37
	Decision Aids	38
	Recommendations/Summary	40

Page

V. Recommendations/Conclusions 47

Introduction 47
Evaluation Criteria 48
Recommendations 57
Conclusion 62

Appendix A: Initial Storyboard A-1

Appendix B: Applicable Enable Screens B-1

Appendix C: Hook Book Notes C-1

Bibliography D-1

Vita E-1

Acknowledgments

This research could not have been accomplished without the help from others. I cannot express my gratitude enough to my faculty advisor, Lt Col John "Skip" R. Valusek, for his undying patience and meaningful guidance throughout the research. I also wish to thank Jacqueline Henningsen (HQ SAC) and Ben Valenti and Capt (USN) John Beaver of the U.S. Navy Damage Assessment Team for their assistance and cooperation during the early stages of this thesis.

List of Figures

Figure		Page
3.1.	Representative Hookbook Notecard	26
4.1.	Document Relation	31
4.2.	Systems Relation	31
4.3.	Assessment Relation	32
4.4.	Stakeholder Relation	32
4.5.	Cryptographic Relation	33
4.6.	Technology Relation	34
4.7.	"Other Areas" Relation	34

List of Tables

Table		Page
1.1.	Compromise Characteristics	6
2.1.	Differences Between DSS and ES	13
2.2.	Methodological Approach to Technology Transfer	18
4.1.	Common Areas of Compromise	30

Abstract

This project researched the adaptive design process and attempted to provide an aid to users who perform assessments of compromised classified information. The background research of this subject did not indicate any previous attempts in solving this problem. Because of this absence of information, the lack of specific guidelines for compromise assessments, and inadequate bookkeeping of information, the scope of the problem was reduced to classified information contained only in documents. The document area appeared to have the most structure and the highest probablility of success.

The adaptive design process started after current operating procedures were reviewed. A storyboard (graphic representations of the system unconstrained by current technology) was depicted and used as a goal for the final system. The storyboard was designed to be "user friendly." Since no off-the-shelf software could be found to implement the storyboard, a redesign of the system was performed.

The "first cut" system used an integrated software package as its foundation. This system relied on a variety of data bases to maintain information pertaining to classified documents. Function menus were used to access other data bases. The system also allows for the entry of suggested improvements, maintained in the "hook book," and provides a notepad function for user convenience.

The system presented is not a final product and should evolve as the problem becomes more defined. The results of this study indicate that further research be conducted utilizing more resources and manpower.

ADAPTIVE DESIGN OF A DECISION SUPPORT SYSTEM FOR COMPROMISE ASSESSMENT

I. Introduction

> **. . one person with the right access may be capable of compromising military systems that cost the United States literally millions, if not billions, of dollars to develop and produce . . . [which] may lead to actions to counter the latest U.S. strategy. And so, from our standpoint, even one case is too many.**
>
> **Britt L. Snyder**
> **DOD Principal Director for**
> **Counterintelligence and Security Policy**

A compromise of U.S. classified information could cause grave damage to the national security. Any U.S. Air Force Strategic Air Command (SAC) subordinate unit which experiences a compromise of classified information must notify Headquarters, SAC when the "probability of damage to the national security cannot be discounted (4:53)." In certain instances, SAC may also be notified if another major command or organization experiences a compromise of a SAC document.

Often, SAC is the originator of the classified materials. When the originator is notified, an evaluation of the classification of the document must be accomplished and an assessment of possible damage performed.

This thesis addresses the fundamental elements of a decision support system (DSS) to aid SAC in assessing the damage caused by a compromise of classified information. This DSS provides: 1) a "kernel"; 2) better documentation in the performance of the

assessment; and 3) standardized procedures for the personnel performing a compromise assessment; 4) a method to allow the DSS to evolve to adapt to changes in SAC's needs.

Background

In recent years, the U.S. has seen a dramatic increase in the number of espionage cases brought to the public eye. As of June 1985, 11 people were accused of spying and were awaiting trial. From 1981 to 1985, 11 others had been charged and convicted of espionage (2:1). Since 1985, other incidents of espionage have been and continue to be recorded.

In 1981, SAC was dealt a serious compromise of classified information. An Air Force missile launch officer, Lt Christopher M. Cooke, was accused of passing secrets to the Soviet Union. He possessed a top secret clearance and had access to various critical documents and operational plans. Neither published estimates of costs nor any assessments of damage to the national security could be found documented in unclassified sources. An erroneous pledge of immunity from prosecution seemed to be at the forefront of the Cooke case. This error appeared to be the reason why the press ignored the damage caused by the compromise and centered their efforts on the conduct of the trial. One can only speculate that the damage was serious enough to force SAC to change various launch codes, documents, and targets.

Most recently the spy ring involving John A. Walker, Jr. and various family members has come to light. This spy ring is suspected of passing Navy secrets to the Soviets for approximately

20 years before detection by federal authorities. Walker was arrested attempting to pass classified documents which contained Navy reports on movements of Soviet submarines and surface ships (16:1). The Walker clan was involved in the theft of a classified document from the aircraft carrier Enterprise which contained information on the Navy's wartime contingency plan for the Middle East. In addition, "keying materials that were used to reprogram top-secret machines that encode and decode classified messages between Navy ships and their land bases" and information about the installation of the Navy's new satellite communications system were stolen. An interesting fact is that wiring diagrams for the cryptography machines were also stolen (1:5). These diagrams combined with the actual keying materials could be reverse engineered and the messages that were transmitted during the active period of the keying materials could be decoded. The extent of the damage to the Navy, other services, and the United States is grave and will probably never be known in totality.

Recent estimates show that over four million people are authorized to handle over 16 million classified documents (13:32). Britt L. Snyder, the Department of Defense Director of Counterintelligence and Security Policy says, these numbers "suggest that we have a greater vulnerability" to Soviet spies (2:32).

SAC maintains large amounts of classified material. For example, two-thirds of the U.S. triad (i.e., intercontinental ballistic missiles and manned bombers) are controlled by SAC. A vast majority of this information involves U.S. war plans. Compromises of this or any related information could seriously impact the

outcome of a future war. SAC also controls many research and development plans for future weapon systems. These plans are extremely important to the national security and often based on technology known only to the United States. Compromises of these plans could also cause grave damage to the national security. Classified material under the auspices of SAC also includes various communications equipment, cryptographic materials, intelligence data, and other assorted documents. This list is not exhaustive. Compromises do not only include espionage cases; classified material temporarily misplaced or lost may also be considered compromised. These facts, coupled with the number of personnel authorized to handle classified material, indicate that SAC is very vulnerable to compromises.

Despite these recent compromises and the vast amount of classified material which exists, it appears that no compromise assessment aids have been implemented or are in the process of being developed in the Air Force or within the Department of Defense. Keyword literature searches through the National Aeronautics and Space Administration (NASA) Scientific and Technical Information Branch, Defense Technical Information Center (DTIC), and manual literature searches did not indicate any compromise assessment aids. Personal and telephone interviews with various Air Force agencies (Aeronautical Systems Division, Air Force Logistics Command, and the Air Force Office of Security Police) who also perform periodic compromise assessments did not reveal any consistent approach to evaluating the damage caused by compromises (3,12,14).

The source which provided the best overall view of compromise assessment, however, was the U.S. Navy Damage Assessment (DA) Task Force. This task force was created in June 1985 as a result of the Walker spy ring. The task force became the controlling authority for the Department of Defense once a compromise (e.g., misplaced or lost classified materials) or espionage (e.g., individual knowingly disseminates sensitive material) has occurred. [The perception of this author is that the task force is not the controlling authority.] The task force then proceeds through a series of phases during the damage assessment process.

One of the initial steps used by the task force is the "fact finding" phase. During this step an investigation is conducted, often by other DOD investigative support agencies, to determine the following:

- Who was involved;
- What was compromised;
- When did the compromises occur;
- Where did the events take place; and
- How was the compromise accomplished?

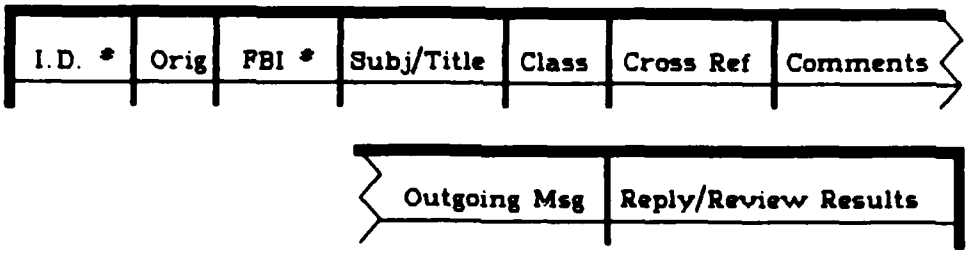
Personnel records are reviewed for the duties held, clearances, access the person had to materials and the types of jobs held. The final phase of this step is to conduct personal interviews to determine what the person was capable of doing and other knowledge of compromises (21).

The second step is to perform a damage assessment. Originators, as well as those organizations which may use similar material, are notified and the impact in various areas are noted: hardware, tactics/operations, training, collection sources and

methods, and Soviet capabilities/vulnerabilities exposed. Also, a determination of lapses, oversights, violations in security, and ways to counter the effects of the compromise are included.

Computer aids are only utilized to maintain a listing of important characteristics for each document compromised. The characteristics of each document are maintained on a spreadsheet with the following headings as shown in Table 1.1. Other than this maintenance of characteristics, no automation of the compromise assessment is performed.

Table 1.1. Compromise Characteristics



1) I.D. # (Identification Number) - the suffix identifying it as either a document (D), message (M), etc.
2) Orig (Originator)
3) FBI # (FBI number) - a number is assigned by the FBI if they ever performed an inventory during their investigation
4) Subj/Title (Subject/Title)
5) Class (Classification)
6) Cross Ref (Cross Reference ID Number) - this is used if there is any involvement with other cases
7) Comments
8) Outgoing Msg - usually to the originator requesting assistance in the compromise assessment
9) Reply/Review Results

The Navy procedures seem to have much more structure than the ones used by SAC. Currently, SAC Security Police Infor-

mation Security Division (SAC/SPI) is notified by various means of a possible compromise of classified information. The originator of the suspected compromised information is then notified and tasked to prepare a damage assessment. The damage assessment is based on a short questionnaire provided by SPI. A subsequent problem arises because the "final" assessment may determine that a review is necessary sometime in the future. That assessment review may not be accomplished by the same individual. Since the assessments do not always follow the same methodology, the reviewer may not understand all the intricacies involved in making the initial assessment. Therefore, the current system utilized by SAC involves individuals making assessments without any specific direction or continuity.

As a result SPI notified the Science and Research Division (SAC/NRA) who in turn notified AFIT of its need for an improved approach. Preliminary discussion of an "expert system" (as envisioned by NRA and SPI) was included with the request. This material included sample menus from which an operator could choose as he determined the specific information compromised. Each menu choice would branch to a successive menu until a final determination of damage was made. As explained in the request, "extensive revision" would be necessary. NRA envisioned this sytem operating on a Zenith Z-150 personal computer.

The specific objectives of the system (as requested by SAC) are:

1) **To help organize the efforts of [functional] experts asked to study compromised documents so they are prompted to systematically study and report on the materials;**

2) To record the results of their analysis in a retrievable and usable form; and
3) To develop the means to assess the cost of a compromised document in real and related costs (8:1).

Objectives

The original request from SAC indicated the need for an "expert system." Although many people have a working knowledge of compromise assessments, none can be considered an "expert." With this shortfall, a decision was made to develop an aid, or a "support system," to compromise assessment and develop this system through learning and evolution. This development process is referred to as "adaptive design" and is discussed in Chapter III. Some highlights, however, are presented here.

To build this DSS, it is necessary to define the problem. From there, a map of the decision process is drawn and a task analysis is performed which identifies the various inputs and outputs the user needs to formulate his decision. This map will take the longest to formulate because of the physical separation of the builder and users. Ideally, this process should take no more than a few weeks.

The individual components of the decision process, or "kernels," may then be identified from the map. The key (central or most important) kernel is selected from these components. This key kernel will be the starting point for building the DSS. Within a few months, the first iteration of the system should be completed. The physical separation, coupled with the availability of the users and hardware/software facilities, may alter this time period significantly.

While the process of choosing a kernel is being performed, the individual components of the decision making process are being graphically illustrated as they would appear on a computer screen. These representations comprise the "storyboard." This starting point is a depiction of what the system ought to do and should be designed without any technological constraints and cost restrictions.

After the first iteration, other iterations of the system design should follow. The amount of time expended should be significantly lower than required in the first iteration. This lower time period is due to the fact that the builder is more aware of the problem than at the outset of the adaptive design process. As more iterations occur, the system should approach the specifications set forth in the storyboard.

The primary goal of this thesis, however, was to initiate a DSS to aid SAC in assessing damage caused by the compromise of classified information. A secondary goal was to research the adaptive design process. This DSS will provide SAC with more efficient procedures and lay the groundwork for an adaptive design process to occur.

The following objectives were satisfied to reach the goal:

1) Design the storyboard for the DSS;
2) Obtain approval of the storyboard from SAC;
3) Develop a kernel system for the DSS;
4) Develop guidance for continued system evolution.

Scope

This research was sponsored by SAC/NRA, but designed to meet the needs of SAC/SPI. It should be noted here that the individual who initially requested the research is no longer associated with SAC/SPI. Because of constant personnel changes and lack of written directives (which would provide continuity), "champions," or principal users interested in the project, were not available. The compromise assessment aid does not assign any system generated cost analysis of the compromised information. Also, because this proposed system is the first of its kind, all work performed on this topic was original and only provides an experimental system using off-the-shelf software to be field tested. Time, physical separation, and technology limitations prevented implementation and evaluation of the proposed DSS.

The majority of the research for this thesis involved defining the problem and learning the fundamental operations of various hardware/software components. The following chapter provides the background for choosing a DSS as an aid to compromise assessment and other systems which could serve as a starting point for its development.

II. Historical Development

A review of the current procedures used by SAC indicates that the system can be improved. Based on SAC's request, the type of system needed would be an "expert assistant (8:1)." An expert assistant can be equated to two types of technology: expert systems (ES) and DSS.

ES evolved from the field of artificial intelligence (AI). Applications of these systems are now appearing in various fields. An expert system works best for a specialized problem requiring specialized knowledge. Ford (7:23) characterizes expert systems as follows:

1) The areas of knowledge have the following prerequisites: the applications are well bounded so the knowledge can be coded into the computer, a human expert is known to perform the task well and is able to develop the knowledge base, and the expert is able to explain the method of solving the task;
2) These systems solve problems by intuition (or "rule of thumb") as opposed to algorithmic solutions;
3) ES use three kinds of information: task specific (data relevant to the current problem at hand), domain specific (relevant to the knowledge base, that is problem solving rules and data), and control (the inferences required to arrive at possible solutions).

The goal of the ES is to provide the user with a decision that is always correct. As Ford (7:24) points out, a satisfactory performance level is one which is close to, at or better than an expert's. Theoretically, the expert system should provide a better solution than that provided by the unaided user.

A DSS can be thought of as an interactive system that uses data and models to solve problems. Ford (7:22) cites four characteristics of DSS:

1) They tend to be used for specified problems that usually face upper-level managers, that is, those problems with no known solutions;
2) They attempt to combine management science methods and traditional data processing functions;
3) They are easy to use by noncomputer people;
4) They are flexible and adaptable to accomodate changes in decision making or problem solving.

A DSS does not operate independently. Rather, this system is used by decision makers as an aid to problem solving. The DSS combines the best of the human mind and computer resources. This combination "produces a total effort greater than that attained by the user and the computer operating independently (7:22)."

No definitions of DSS and ES are universally accepted. A useful and succinct working definition was provided by Valusek in which he describes a DSS as a "system (automated or manual) that supports the cognitive processes of judgment and choice (21)." In fact, an ES has been called an intelligent DSS (19:138). Turban (19:141) summarized the differences between ES and DSS as shown in Table 2.1. While none of the definitions are exactly alike, inherent in all of them is the idea of an expert. Whether the individual is called an expert, upper-level manager, or decision maker, the fact remains that a knowledgeable individual should be available to direct the task.

Table 2.1. Differences Between DSS and ES

	DSS	ES
Objective	Assist human	Replicates (mimic) human and replace him/her
Who makes the decision?	The human	The system
Major Orientation	Decision making	Transfer of expertise (human-machine-human)
Query direction	Human queries the machine	Machine queries the machine
Clients	Individual and/or group users	Individual user
Manipulation	Numerical	Symbolics
Problem area	Complex, integrated, wide	Narrow domain
Data-Base	Factual knowledge	Procedural and factual knowledge

Note. From "Integrating Expert Systems and Decision Support Systems" by Efraim Turban and Paul R. Watkins, 1985, Decision Support Systems: Putting Theory Into Practice, edited by Ralph H. Sprague, Jr., and Hugh J. Watson, p.141. Copyright 1986 by Ralph H. Sprague, Jr., and Hugh J. Watson.

Research has not uncovered any related systems in the Air Force (3,12,14). The idea of a compromise assessment aid is new to SAC. Surprisingly, during personal interviews, a few organizations actually expressed resistance toward an improved, automated system. One organization did not foresee a need for any computerized system. The rationale was that the organization rarely performed any compromise assessments (3). Another organization felt the problem faced by SAC was merely a "management problem" and better procedures would solve the problems at SAC (14). This organization also indicated the number of assessments performed did not warrant a system. The former organization provided a good argument. A new system could waste money or time if it is rarely used. The latter organization, one

which deals with many modifications to current and future USAF weapon systems, by its charter would seem to have more compromises than they seem to admit. This "sensitivity" problem was realized early in the research as a potential stumbling block (8:1). The management argument posed is unfounded. In fact, the willingness of management to identify a problem and improve their procedures is an indication that they are performing their job. However, since no expert could be found nor were any compromise assessment aids found in the USAF, analogous technological fields were researched to determine common areas and possibly use those technological fields as starting points in the research.

Related Research

A system which initially resembled that envisioned by SAC is being used by the Environmental Protection Agency (EPA). The Expert Disclosure Analysis and Avoidance System (EDAAS) is an ES which is being used to screen Freedom of Information Act requests. The EPA maintains sensitive information, provided by chemical manufacturers, importers, and processors, which forms the basis for the EPA's evaluation of health and environmental risks (6:72). This confidential business information cannot be released directly to the public and poses a problem for the EPA information officers. A decision has to be made about what information may be released without compromising other sensitive company data by the information officers.

The EPA compromise of sensitive or classified information is similar to that of SAC. Direct release of sensitive information is not acceptable. As with SAC, the release of information which could be combined with other available information to estimate sensitive information is also not acceptable.

The solution to the EPA problem was an ES. This ES "emulated" an industry analyst who, acting as an espionage agent, uses the data from the proposed release of information and estimates corporate operations and strategies. These results would then be evaluated against Federal regulations, and a determination made concerning its release. In addition, reasons concerning the ES decision would be provided (6:72). EDAAS has been hailed as an effective ES. This system, which uses two knowledge bases and two inference engines, took "four staff-years" to develop (6:75). Feinstein claims the system makes no mistakes and does the work of ten professionals (6:84).

However, EDAAS was abandoned as a starting point for this thesis for several reasons. First, the builders had the luxury of emulating the decision processes of an industrial analyst and a legal advisor. The SAC problem, as discussed earlier, could not be referred to an expert. Second, although the laws concerning disclosure of confidential business information were vague, this ambiguity was overcome by including all parties interested in EDAAS in the planning process. All of these groups then provided inputs on how the system would make decisions (6:76). Again, the lack of experts and the inability to include all interested parties in SAC affected the decision to not model the system after EDAAS.

Finally, the problem faced by EDAAS involved reasoning which utilized actual production quantities (stored in a data base) to perform various calculations. These calculations were compared against constraints established by the planning group. SAC does not have a data base that relates to compromise assessments and much of the data which would be used is not quantifiable. The decision to abandon EDAAS was made primarily on the fact that no part of the SAC problem could be reduced to simple numbers.

Another process researched was environmental impact assessments. On the surface, the preparation of environmental impact statements seemed to correlate to that of compromise assessments (15). In a sense, the two fields have the same problem. Both are manual; however, environmental impact statements are required to include discussions in specified areas (5:22) whereas no specific areas of damage assessment are specified for compromise assessments. The only requirements specified by SAC are that the following general topics be discussed:

- Currency/accuracy
- Relationship to SAC Weapon Systems
- Effect on SAC Weapon Systems
- Assessment
- Recommendations

This idea of specific areas will be carried over into the design of the DSS. All compromise assessments do have common requirements which will be specified later in the thesis.

Another analogous process, technology transfer, provided some useful information. Spencer calls technology transfer the "planned and rational movement of information and techniques on

how to perform some tasks, simple or complex (17:29)." The most useful defined approach to technology transfer was developed by the Office of Science and Technology and the Mitre Corporation (10:119). This approach consists of the major steps required and checklist actions for each step. Table 2.2 shows the major steps and general areas which the checklist actions encompass.

Overview of the DSS Design

The main goal of this research was to initiate the adaptive design of a DSS to assist in damage assessment. Introduced by Keen (Keen:15), the adaptive design process focuses on "getting finished" through an "adaptive process of learning and evolution." The major players in the system include the user, builder, and the system itself. The interaction of all these links, referred to as "adaptive links," provides the framework of adaptive design.

The SYSTEM→USER link emphasizes user learning while the USER→SYSTEM link provides the requirements of the user to the system. The USER⇄BUILDER loop is the insurance that the user drives the design process and a quick delivery of the initial system is accomplished. The BUILDER⇄SYSTEM loop, perhaps the most difficult of the three to discuss, provides the system the ability to accomodate new functions or capabilities as required.

This research project provides SAC with an initial aid to compromise assessment. Keen felt that if the adaptive design framework was valid, "then Decision Support is a meaningful and independent discipline (11)." This research will also attempt to validate the concept of adaptive design as a useful tool.

Table 2.2. Methodological Approach to Technology Transfer

METHODOLOGICAL APPROACH DEVELOPED
BY THE OFFICE OF SCIENCE AND TECHNOLOGY/MITRE

SEVEN MAJOR STEPS IN MAKING A TECHNOLOGY ASSESSMENT

STEP 1	**DEFINE THE ASSESSMENT TASK** Discuss relevant issues and any major problems Establish scope (breadth and depth) of inquiry Develop project ground rules
STEP 2	**DESCRIBE RELEVANT TECHNOLOGIES** Describe major technology being assessed Describe other technologies supporting the major technology Describe technologies competitive to the major and supporting technologies
STEP 3	**DEVELOP STATE-OF-SOCIETY ASSUMPTIONS** Identify and describe major nontechnological factors influencing the application of the relevant technologies
STEP 4	**IDENTIFY IMPACT AREAS** Ascertain those societal characteristics that will be most influenced by the application of the assessed technology
STEP 5	**MAKE PRELIMINARY IMPACT ANALYSIS** Trace and integrate the process by which the assessed technology makes its societal influence felt
STEP 6	**IDENTIFY POSSIBLE ACTION OPTIONS** Develop and analyze various programs for obtaining maximum public advantage from the assessed technologies
STEP 7	**COMPLETE IMPACT ANALYSIS** Analyze the degree to which each action option would alter the specific societal impacts of the assessed technology discussed in Step 5

Note. From Society and the Assessment of Technology (p.119) by François Hetman, 1973, Paris: Organisation for Economic Co-operation and Development. Copyright 1973 by Organisation for Economic Co-operation and Development.

Because an ES was initially requested by SAC, the rationale for the decision to use a DSS, instead of an ES, was presented in this chapter. The development of an ES should not be considered until the area of compromise assessment becomes more structured and experts emerge. Other systems which were researched, as possible starting points, for the adaptive design of the DSS, were also included for background. The following chapter builds on the information presented in this chapter and discusses the methodology used to develop the DSS adaptive design process to be presented to SAC.

III. Methodology

The following four objectives (as discussed in Chapter I) provide a course of action toward the enhancement of the compromise assessment problem faced by SAC:

1) Design the storyboard for the DSS;

2) Obtain approval of the storyboard from SAC;

3) Develop a kernel system for the DSS;

4) Develop guidance for continued system evolution.

These objectives can be revised into a format compatible with adaptive design. Briefly described in Chapter II, the adaptive design process allows the system to evolve and can be represented by the following processes: 1) Problem Definition; 2) Kernel Identification; 3) Storyboard; 4) Kernel Development; 5) Evolution.

Problem Definition

Guidelines for the assessment of compromised information are outlined in Air Force Regulation (AFR) 205-1, Information Security Program Regulation. These guidelines are very loosely defined and are a source of the problem in performing any assessment. The original classifying authority, once notified of a compromise (usually by SAC/SPI), is required to review the information involved in the compromise and determine whether:

> (a) The classification should remain at its current level without changing any information;
> (b) Any part of the information should be modified to minimize the effects caused by the compromise, without any change of the classification; or
> (c) The classification needs to be modified (4:23).

In addition, if the information falls into categories specified in (b) and (c), the user should give notification to all holders of the classified material that a compromise has occurred. If a compromise occurs, the person performing the assessment must also determine if related classified information is affected. If the information is affected, then the classifying authority of the related information determines whether the information can be applied to any of the above categories.

The existing procedures at SAC appear to comply with the intent of AFR 205-1. Based on the current procedures, the original classifying authority (used in AFR 205-1) is synonymous with the user (described in this research). The user will be the individual assessing the damage of the compromise. The objectives of the user were tasked by SAC/NRA in their initial request for assistance [see pages 1-7 and 1-8] (8:1).

It became evident that a wide variety of information could be compromised. An initial study of the problem indicated that compromises could occur in three main areas: technology, documents, and personnel. The technology area consisted of actual equipment which could be compromised or lost to the enemy. Documents are self-explanatory. The personnel area deals with cases of espionage where the individual(s) compromised information or information from any of the other two areas. If it found that this espionage revealed information from the technology and document areas, the assessment would also be performed using the same procedures for these areas.

A top-down analysis of these areas indicated the entire problem could not be managed through this research; therefore, a decision was made to limit the problem to the area of documents only. The rationale for this decision was that personnel and technology could be analyzed using the same approach as that used for documents. Also, assessment of the document area appeared to have the most structure which would allow for a more substantial kernel and provide a better chance for initial success.

Each compromise assessment seems to be so unstructured and different, no universal rules could be established. The compromise assessment requires judgment and choice. Many of the responses during the assessment are based on the user's judgement. At the same time, the system needs to allow the user the option to query various sources to make a choice. Different users may use different information to make decisions: one may use an estimation of the dollar cost to change established procedures; another may judge the loss solely on the type of information compromised. The problem is, therefore, to develop an aid for users when performing a compromise of a classified document within the guidelines of AFR 205-1 while supporting the judgment and choice of the users.

Kernel Identification

Based on the problem definition, a map (see page A-1) of the decision process was formulated. The map was formulated from a variety of sources. Key aspects of SAC, the Navy, and technology transfer procedures were considered when building the map. From this map, a task and data analysis was performed.

As a result, this map appeared to be an accurate representation of the decision making process. The individual components of the decision process, or kernels, were then considered for the storyboard.

Storyboard

To capture the essence of the compromise assessment process used by personnel, a series of physical representations (i.e., computer screens) were designed. These representations are actually characteristic of the representations, operations, memory aids, and control mechanisms (ROMC) approach specified by Sprague and Carlson (18:96). The representations aid the user by helping conceptualize and communicate the problem. The operations are the functions which manipulate and analyze the representations while the memory aids link the representations and operations. The control mechanisms manage the entire system.

The storyboard presented (Appendix A) was an initial attempt at capturing the tools that could be used in the decision making process of the users. A structure of the document assessment problem is also included. An assumption was made that the user will already have entered pertinent information concerning the compromise (e.g., title or number of the document, the classification of the document; a control number of the assessment; and user/office symbol of the individual preparing the assessment). If, for example, a document were discovered to be compromised as a result of an espionage case, a description of the circumstances

and of the espionage agent would already be accomplished prior to entering the document portion of the process.

The system proposed by the storyboard would only be used for the analysis of one compromised document at a time. For multiple compromises, the system would probably be linked by the name of the person responsible for the document, or the office of primary responsibility (OPR). It could also be linked by relations to other assessment control numbers. Among the features of the proposed storyboard system are :

- A menu bar which contains titles of different menus would line the top of the computer screen. When the mouse input device cursor is placed on the title of the menu, the user could "pull-down" to commands listed in the menu.

- At any point of the assessment, the user would be able to request a summary of the assessment up to that point as well as a hard copy printout through the use of a menu.

- Specialized "Help" windows also accompany each screen aiding the user in interpreting directions specified by the system.

- If the user has any questions with respect to other assessments or wishes to scan related assessments, the query can be accomplished with the possession of a valid authorization code.

- An editing function allows the user, again, through the use of "pull-down" command menus, to move through the tree, in reverse, to change any responses previously entered.

Kernel Development

The description of the system defined by the storyboard cannot be fully implemented using off-the-shelf software. One of the risks in designing a storyboard is that the ideas represented cannot always be mapped into the actual system. Concessions were made in the features so an initial system could be developed using off-the-shelf software. Based on the storyboard, a technically feasible kernel system was identified and developed with the adaptive design process in mind. This kernel system is flexible enough that the design is easily modified, allows continuing interaction between the builder and user, and is inexpensive. Many of the features specified in the storyboard were not implemented. The kernel system uses a database program as its basis. A full discussion will be presented in Chapter IV.

Hook Book

The hook book is a compilation of notes and ideas on the future evolution of the DSS proposed. To further reinforce the idea, all relevant information of the conditions under which the idea was formulated should be noted. For example, an idea may be generated while reading a newspaper article. Figure 3 1 shows an example of a hookbook note made on an index card. The entry in the hookbook should include, at a minimum, that the newspaper was being read, the date, what the improvement is, and what made you think of the system. Ideally, the recording of notes should be performed religiously; however, human nature often takes control and notes are often incomplete and illogical.

Regardless, many entries were made while the system was being built. Some of the ideas were implemented, others were considered for future implementation.

DATE: 9/27/86
IDEA: Ease of notepad operation
CIRCUMSTANCES: After working on the Apple
Macintosh, it seems to be a pretty good idea
to have a mouse pointer/input device to select
the NOTEPAD function from a pull down menu.
A small "sheet" of paper overlaps the current
screen and the note is entered. To close the
function, the pointer is placed in a small box
provided. The original screen is then displayed.

Fig. 3.1. Representative Hookbook Notecard

Evaluation

An area of DSS which is often overlooked or ignored is the evaluation phase. Evaluation plays a critical role in the continuing evolution of the DSS. This information could indicate the acceptability of the system by the users or impact of the DSS on the decision making process. If the system provides no useful changes, the system will ultimately wither away. Discussion on some criteria for evaluation are discussed in Chapter V.

This chapter provided discussion on the methodology used in developing the system. By using the adaptive design approach, a

system can be developed which is initially beneficial to the user and has the capability to evolve into a better system. Even if the system is not implemented, this analysis provides structure to a previously unstructured problem. The next chapter discusses the initial prototype, or "kernel" system.

IV. Resulting System

The intent of developing a kernel is to provide a starting point for the evolution of the system. It must be reemphasized that no known attempts have been made to develop a compromise assessment aid. Also, no automated data base information on compromises of classified material was available. Because of these shortfalls, the kernel system designed only "scratches the surface" of compromise assessment.

Computer Systems

Since SAC requested that the system designed be able to run on an IBM-compatible personal computer, the Zenith family of personal computers was deemed acceptable. Because of the delays which accompany the procurement of software, the decision was made to use a software program already owned by the Air Force Institute of Technology (AFIT). Programs, such as Lotus 1-2-3 and dBase III were reviewed as possible candidates. The software program Enable by The Software Group was eventually chosen to design the kernel system.

Enable has the ability to handle a wide variety of tasks and functions. For the long term, the graphic capability of the software was extremely appealing. This capability was seen as a benefit to improve the capability as the needs of the users change and the system evolved. For example, as the ability to determine the costs associated with a compromise evolve, bar/pie charts, possibly associated with a cost data base, may aid the user's decision mak-

ing process. Also, the ability to easily create menu choices, customize input forms, and easily retrieve data from files influenced the choice of Enable. Other functions provided by Enable, but not considered for use, include word processing, spreadsheet, and telecommunications.

Initially, an attempt was made to use the Z-150; however, the lack of a hard disk made Enable extremely difficult to operate. The main Enable program consists of four disks: System, Operation, Utility, and Tutorial. The Z-150, which has two disk drives, calls for a constant "swapping" of these program disks. This swapping was seen as "user unfriendly" and could lead to the system being rejected by the users. Because of this shortfall, the Zenith Z-248 with a hard disk was chosen as the primary computer system.

Data

The initial task was the determination of the information to be used by the system. The spreadsheet information gathered by the Navy DA task force was extremely helpful. While their system is used on a case-by-case basis, it can be extended to multiple cases. The Navy spreadsheet also did not involve subjective data: it was used only as a bookkeeping tool and not as a decision aid. The checklist for making a technology assessment (Table 2.2) provided useful ideas in determining important aspects related to compromise assessment. An analysis of the storyboard indicated there are many pieces of information that were common to all compromise cases. These common areas are listed in Table 4.1.

The next task was organizing these common areas in an efficient manner to be used by the system. Certain areas are related to others, called a relation. Each instance of a relation can be considered a record and a collection of these related records constitutes a data base. All of the different data bases are related through the use of the compromise assessment case number. This number is the control number assigned by SAC/SPI at the start of the assessment.

Table 4.1. Common Areas of Compromises

Compromise Number
Date of the Assessment
Document Number
Office of Primary Responsibility (OPR)
Date of the Document
Classification
Stakeholders
General Area of Compromise
Damage Caused by Compromise
Systems Involved
Review Date
Description

Figures 4.1 through 4.7 depict the relations used in the system. Figure 4.1 shows the fields in the document data base. The information does not require any decisions or assessments to be made by the user. All information entered into the system would be "hard" data based on the characteristics of the document.

Many of the assessments will involve some type of system (e.g., weapon systems). A means to record this data was devel-

oped by relating the system with the compromise number. Figure 4-2 is a representation of this relation.

The assessment data base contains most of the subjective information concerning the case. A majority of the cases would use this relation to enter data. One of the more important fields is the damage field. This field will, at a glance, indicate the importance of a particular assessment. The review date can be used by the system manager to determine which compromises are due for a review by simply performing a search. Figure 4.3 lists the relation.

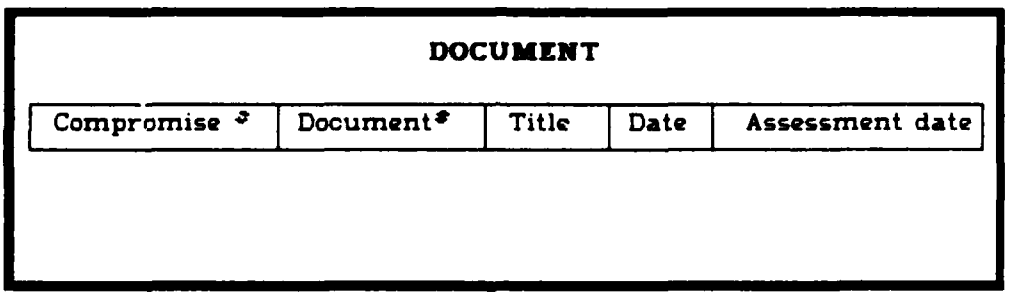


Figure 4.1. Document Relation

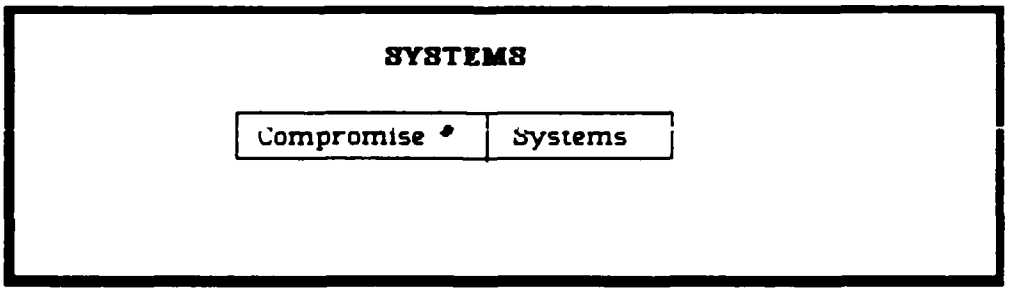


Figure 4.2. Systems Relation

The stakeholder data base is seen as a powerful tool once the data base is established. A listing of the relations is found in Figure 4.4. A stakeholder can be described as an organization, friendly or enemy, who will be affected by the loss of a classified document.

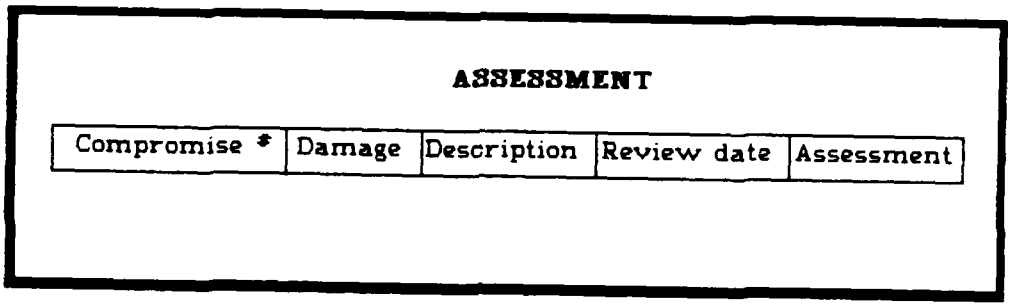


Figure 4.3. Assessment Relation

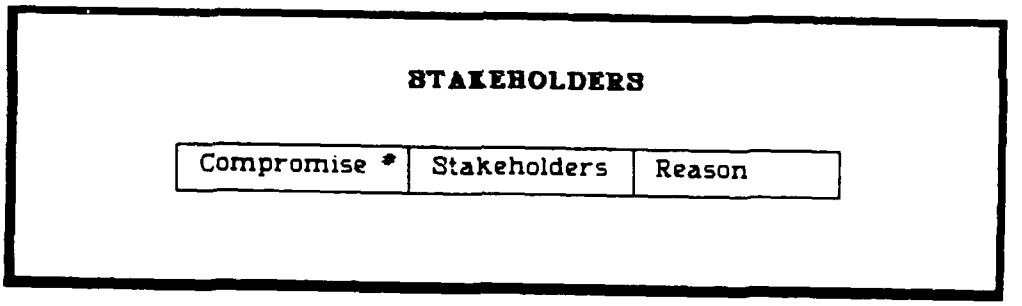


Figure 4.4. Stakeholder Relation

A vital piece of information which is to be added along with the stakeholder is the rationale for the entry. The rationale for certain decisions seems to be the missing link in subjective decision making. It will become valuable in future assessments so other users can understand the logic of past assessments. In addition, users will learn from mistakes or omissions that occurred in previous assessments.

Compromises of cryptographic materials poses many additional problems for the person performing the assessment. These documents are often used to transmit classified information from one unit to another over nonsecure lines of communication. Usually the document is in effect for a specified time period and then superseded. By listing all messages which may have been compromised during that time period, the user can use that list as a reminder to perform an assessment on those messages. Figure 4.5 provides the relation for the crypto data base.

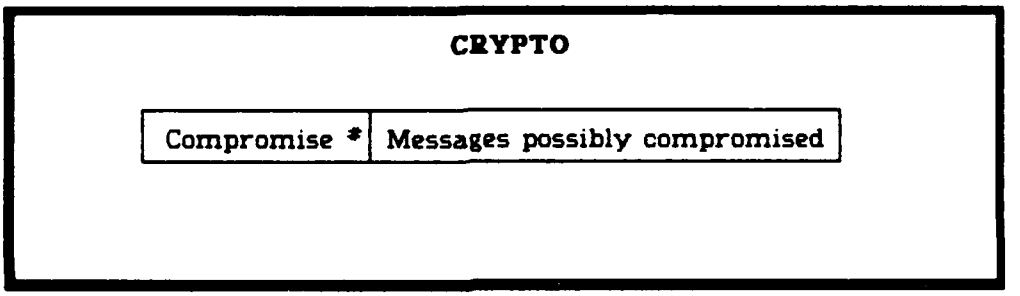


Figure 4.5. Cryptographic Relation

Figure 4.6 shows the technology relation. As in Figure 4.1, a particular document may require more than one entry. In this case, there may be more than one related technology. This data base accomodates multiple entries by use of a common case number. A subjective data field is provided in this data base to discuss the impact that a particular technology may have when that knowledge is lost.

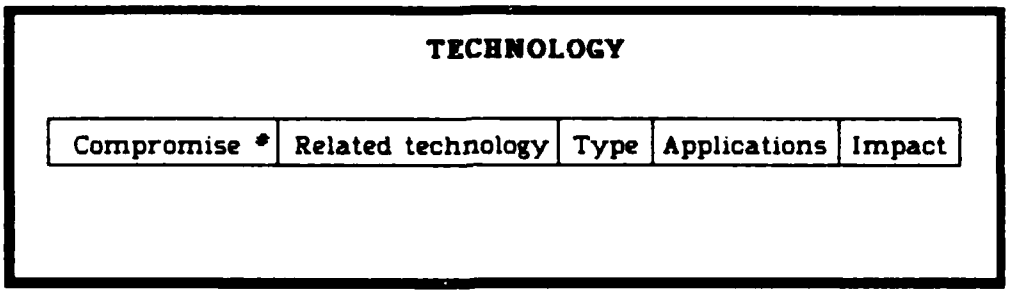


Figure 4.6. Technology Relation

If the information compromised did not fall into the cyrpto or technology fields, the user could input any additional data here or query other records to determine any common elements to other cases. The relation is listed in Figure 4.7.

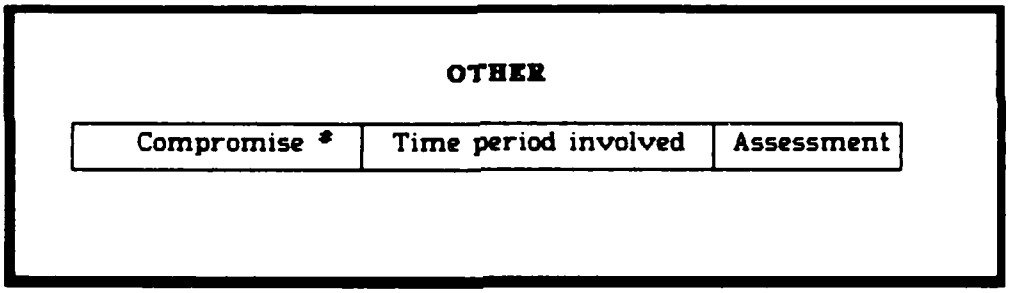


Figure 4.7. "Other Areas" Relation

System Operation

The control aspects of the system were created through the use of macro programs. The ability to easily create macros greatly aided in the development of the system. Because the macros are keystrokes stored in memory, functions normally performed by the user can be initiated and performed with very little effort. In conjunction with the macros, menus were created

to allow the user to easily execute them. These two features, along with the data bases, comprise the kernel system.

Once Enable has been activated, the Sign On Screen is displayed. [All Enable screens discussed are depicted in Appendix B.] At this point, the user should ensure the time and date are correctly entered. The system uses this data later in the assessment. This function will be discussed in detail later in the thesis. From this screen, the Main Menu is accessed.

The Main Menu is the starting point of the system. All functions normally performed by Enable are still available. By accessing the menu which is associated with the Master Control Module (MCM), the compromise number, which is assigned to the case, is entered. The MCM is the controlling program which integrates the system. The compromise number, when entered, is maintained in the MCM for future use and remains there until it is intentionally changed by the user. Once this number is input, a macro is initiated.

This macro sends the user to a screen where data on the document is input. The macro is written so that the screen "freezes" until the input form is displayed. During this time, the system calls the ADD command, finds the document database, and displays the default form. This form was created and specified as the default form at the same time the data base was designed. The macro also automatically enters the compromise number on the input form, reducing the number of keystrokes required of the user.

The data is entered through the use of one of two macros. As discussed earlier, certain areas may require multiple entries. If multiple entries are not required, one macro will enter the data and close the document data base, returning to the DBMS Command Chart. If multiple entries are required (e.g., Systems), the other macro enters the data into the data base. Following the entry of data, the system calls the MCM for the compromise number that was entered at the start of the session. The current compromise number is then automatically entered on the next entry form. With a minimum break in continuity, the user is then only required to input the next entry. The use of a macro here is seen as one of the keys in developing the system. It was felt that the more keystrokes accomplished by the user during an assessment, the less interest the user will have in the system.

Another feature of the system is the ability to open a second data base while active in another. This feature is accomplished with a customized menu. The menu lists the other data bases by number, for example "4 - ASSESSMENT." When the user calls up this menu, the option can be selected by using the cursor to select the option or depressing the number preceding the data base (in the example, "4"). As each menu choice is "highlighted," a window describing the function is displayed.

When the selection is entered, a macro is initiated. As in the case of all macros utilized, a function to freeze the screen until all actions are complete was included in the macro code. The data on the screen is saved and the system returns to the DBMS Command Chart. At this point, the system is able to call

the MCM to open a new data base. The data base is determined by the menu choice while the displayed input form is automatically linked to the data base selected. When the call is made to the MCM, the compromise number is again recalled for automatic entry on the form.

Additional Functions

In addition to the ability to access other data bases, other functions are provided in the "add" mode. If the user will be working multiple assessments in the same session, the user is able to enter a new compromise number. The compromise number is changed by displaying the menu and selecting "COMPROMISE NUMBER." The new number is typed into the box provided in the menu. When this number is entered, it is sent to the MCM to replace the old number.

Secondly, the user has access to a "notepad" function. The intent of the notepad is to serve the same purpose as a pad of paper and pen. By accessing the notepad through the main menu, the notepad data base is opened. The date and time are automatically displayed and only the user's comments need to be entered. The subjects of the comments are not restricted to any particular areas. The notepad is provided only as a convenience to the user so that ideas and "snapshot thoughts" can be recorded with minor interruption of decision making actions. At the end of the session, the user can gather the notes from the data base and accomplish further actions as required. For example, a user may be unsure if one system is actually affected by a specific

document. He may have to perform further research and return to the assessment. The notepad function will allow him to record his thoughts. To return to the user's previous actions, a selection made from the main menu will return the system to the data base and compromise number previously displayed. The notepad is seen as an important decision aid for the system. While its concept is trivial, the user can use it as a memory aid to assist his decision making process. The amount of effort required to access this function is seen as a benefit because the user's train of thought is minimally interrupted.

A function similar to the notepad is the hook book. Discussed briefly in Chapter III, the hook book is a list of notes which are used to comment about the current status of the system and suggested improvements to the system. The hook book also has its own data base. It is opened using the same method as the notepad and the system also automatically enters the date and time. The hook book is closed using the main menu. Because this is a multi-user system, the hook book is intended to maintain suggesstions from all users. The person maintaining the entire system, or "system manager," will take necessary actions to filter and implement (when possible) the suggestions entered into the hook book.

Decision Aids

The system described is not seen as much of a benefit to "early" users of the system. The early users will be entering data on compromises, however, they will be laying the groundwork to

be used by "later" users performing compromise assessments. In other words, as more data is entered from previous assessments, the user can use that data to make better decisions on the impact of a compromise. The early users will have to rely on their own ability to assess the damage.

Since no data bases have been established nor have written procedures been established by any higher headquarters, the individuals tasked to perform a compromise assessment are not aware of the information contained in previous assessments. This problem is alleviated with the ability to access other assessments. Through the use of a customized menu (different from the one previously discussed), the user has the ability to easily query other data bases for related information.

The menu looks similar to the one which accesses other data bases for entry of data, however, different macros are executed when the corresponding menu option is selected. Generally, all macros used in this menu perform similar functions. When an option is selected, the screen is frozen until all actions are accomplished by the system. The data on the screen is saved and the system returns to the DBMS Command Chart. The DISPLAY function is then selected and the appropriate data base is automatically entered based on the option selected. The user may or may not enter conditions on which to search the data base. If the user does not enter any conditions, the entire data base will be displayed. If the user enters conditions, the system will only display those records which match those conditions. The system provides the field names and the available operators at the bottom of the

screen to conduct the query. For example, the stakeholders data base may be queried for entries which refer to SAC/NRA by entering "STAKEHOLDERS EQ "SAC/NRA"."

Occasionally, data in a field may not be known or the field may be too lengthy to enter. Through the use of "wild card" symbols (i.e., "$" and "?"), the user may easily scan an entire field. Using the above example, the query can be made by typing "STAKEHOLDERS EQ "SAC?"." The power of this tool can be seen when fields can contain 254 characters. These fields are often used to contain written text concerning the compromise. If records contain important keywords (e.g., espionage, lost, misplaced, SAC, TAC, etc.), the user can easily scan these fields using keywords and wild cards. For example, a query for espionage assessments is performed by entering "ASSESSMENTS EQ "ESPIONAGE"."

Recommendations/Summary

This chapter provided discussion on the resulting system designed. The design was based on ideas from various sources not necessarily involved with compromise assessment. The resulting system falls short of the storyboard due to one key fact: the decision to use off-the-shelf software limited the capabilities of the system. If the manpower and resources were available, programmers could have developed software to support the functions depicted by the storyboard. Because of the inability of the software to perform in accordance with the envisioned system, other shortfalls occurred.

Adaptive Design of System. The hook book is an effective tool to document features (i.e., requirements determination) which should be considered in future iterations of the DSS design. Because of time and technological constraints, these ideas were not implemented in the system. As this research progressed, it became evident that the hook book is better tool if it is used as a diary. This is important if a new builder is put into place and a record of past failures and reasons for failure are required. The log will prevent others from wasting time attempting to implement an additional DSS feature using a previously failed technique. Following are hook book entries for the continued evolution of the system.

Report Generation. An appropriate format for the final assessment needs to be determined. The final assessment would benefit from the report generation capabilities of Enable. The report could be used as a hard copy record of the assessment. The problem, however, is compiling information from different data bases keying on the compromise number.

On-Line Help. As the system evolves, the help provided in the information block will become less important to the user as he becomes more familiar with the system operation. Eventually, this information should be moved to an on-line help function. If the information currently in the system is insufficient, additional information should be included in the "help" function.

Current Record. One of the current problems with the resulting system is working with the current record. When

another function is entered (i.e., notepad and hook book), the current record must be saved and then the new function can be displayed. The problem arises when trying to return to the saved record because there is no method which limits keystrokes by the user. While the compromise number is stored in memory, if a particular assessment has multiple entries in one data base, the system cannot automatically access the last one saved. In this case, the user must specify the conditions exactly to find the last record entered.

Data Entry Limitation. For all data bases, each data field is limited to 254 characters. Currently, if the 254 character limit is reached, that information must be entered and the remaining information is treated as a separate record. A way to link these data bases needs to established. The original storyboard envisioned a system which allowed integration with a word processing program. Thus far, no efficient method to fully integrate the word processing and data base functions could be performed.

Window Limitations. The data base functions require the window, or presented screen, to fill the entire computer screen. Some of the other functions in Enable, for example, the spreadsheet function, allows windows to be reduced for display. This reduction allows multiple windows to be displayed, therefore, more information can be presented from different sources. In retrospect, the spreadsheet function may serve the purposes of this problem better than the data base function because of the window limitation.

Multiple Specifications. The query function allows the user to search a data base to find records which meet specified conditions. The system does not allow the user to specify multiple conditions to determine if they are shared by the same assessment. The system would provide more decision support if it could access more than one data base simultaneously.

Automatic Access. The system should be able to detect specific entries made by the user and based on these entries, access other functions as required. For example, if the system recognizes entries similar to a previous assessment, the system could automatically signal the user that a pattern has been recognized. The user would then be able to use the information from the other assessment as he chooses.

Mouse Input Device. A mouse input device greatly reduces the need for "computer literacy." The mouse replaces cursor control and allows easier access of menus. Many keyboard functions can be accessed without knowledge of specific keystrokes. One of the better mouse devices is on the menu driven Apple Macintosh. Incorporation of an input device similar to the Macintosh would be extremely beneficial to the system.

Expansion of Kernel. The system was designed to accomodate only compromises of documents. The system eventually needs to be expanded to accomodate all areas of compromises. The documents area was chosen for the kernel system because its structure appeared to provide a high probability of success. The other areas appeared to have less structure and, therefore, their decision processes are expected to be more difficult

to capture than the document area. Expansion of the kernel will be extremely challenging.

Keystroke Recording. Keystroke recording may provide new insights into the decision process of the user. An analysis of the keystrokes of many users may allow for the development of a conceptual map. This conceptual map may help in future compromise assessments.

Password System. The data base is currently open to all users. The security level of the information contained in the data bases may not always be consistent with that of the user. Access to classified information is based on possession of the appropriate security clearance and a need to know. If the user does not have access, some measures must be built into the system to restrict access to the data.

Interservice Queries. One measure of effectiveness to be evaluated, discussed earlier, dealt with information sharing. If the user has the ability to request information from other services, he is likely to make a better decision. One of the keys is interoperability. If the current communications problem between the services is any indication, the interoperability of compromise assessment systems (assuming other services automate their compromise assessments) will not occur in the near term.

Cost Analysis. One of the key points in an assessment is to determine the cost associated with the fix of the damage caused by the compromise of classified information. The cost not only includes the cost to the U.S. but also the benefits received by the other side. Costs to the U.S. can take on a variety of forms

(e.g., the dollar value to change compromised cryptographic codes, the amount associated with changing training procedures, etc.). Benefits to the enemy may include the amount saved by receiving U.S. classified technology, thereby saving research and development costs. One suggestion for determining these costs would be to construct, if not already constructed, a large data base which houses current costs associated with all USAF functions (e.g., amount to retrain bomber crews). Projects and the areas which were used in supporting the completion of that project would be programmed into the DSS. The DSS would detect a pattern in the compromise and determine what fixes were needed. The fixes would then be compared to those functions programmed into the DSS and the system could estimate the cost of the compromise.

Summary. The representations illustrated in the storyboard could have been generated on the screen of the system. However, user interface could not be effectively handled. For example, the system represented by the storyboard would send the user to another part of the assessment simply by clicking a mouse input device in a specified area (which initiates a macro). In order to initiate a macro in the system described, the user must perform several keystrokes. User friendliness suffered as a result of using off-the-shelf software. The trade-off for lower costs (i.e., dollars to buy the system and time expended to design the system) was the inability of the system to perform functions specified in the storyboard design. If further user friendliness is to be pursued, additional funds and manpower should be directed to this area. Despite these shortfalls, the resulting system will be used as a

starting point in developing a more complex system. The next chapter provides guidance for the evolution of the system.

V. Recommendations/Conclusions

Introduction

The assessment of compromised classified information is by no means a trivial matter. The ideal situation would be a total elimination of compromises. Unfortunately, this solution is not realistic. This thesis started with the premise that compromises will occur and continue to occur. The problem is, once a compromise has been identified, what to do next. The resulting system described is only the beginning of the solution to a complex problem. This chapter will provide guidance on the continuing evolution of the system and its components.

While originally researching the topic of compromise assessments, it became evident that this problem area had no structure. Personnel had only rudimentary guidelines (specified in AFR 205-1) when performing assessments. Through the interviews and research performed, the common areas of an assessment were determined. From this information the system was developed as described in the previous chapter. This system is seen as providing some structure to a previously unstructured problem. The data fields in the various data bases serve as memory aids to the users when entering information. This data can now be collected and organized in a manner which is useful to all users.

The primary goal of this thesis was to provide a decision tool to aid SAC in performing assessments of compromised classified information. The system described is not a final system, nor was it intended to be. Because this area has not been previously

explored, the starting point of this thesis was the problem recognition. Time constraints and, to a certain extent, technology constraints prevented the implementation of a usable system. This thesis did, however, provide a preliminary design for an aid to compromise assessment.

The secondary goal of this thesis was to research the adaptive design process. The builders of a system rarely understand the users' needs and the users may not completely understand what they want. From this initial system, users may levy additional requirements and specify additional features. This user feedback should be an ongoing procedure. To aid this procedure, a framework for the evolution of the system will be provided as well as organizational requirements for this evolution. The section Evaluation Criteria and Recommendations provides guidance on the adaptive design of the system.

Evaluation Criteria

The evaluation of the system can be as important as the system itself. In fact, developing the evaluation criteria may be as difficult as building the system. For this reason, evaluation is often ignored or overlooked by all interested parties. If the system is not perceived by the users as beneficial, it will not be used. If the system is not meeting the expectations of all stakeholders, then the reason must be determined. Throughout this research, evaluation criteria were documented. These criteria have been divided into four areas: prior to the initiation of assessment, during the assessment, after the completion of the assessment, and over the

long term. Following is a discussion on these four areas, measures for evaluation, and problems with the evaluation criteria.

Prior to the Intiation of Assessment. The main purpose in conducting part of the evaluation prior to the assessment is to get a user's perceptions of the overall decision process and of the system operation before any work is done. An attempt was also made to minimize user distractions. Any distractions to the user, while making a decision, may actually discourage use and doom the system. Five criteria have been targeted for this portion of the evaluation.

Manual Completion Time. The time in which an assessment could be completed, without the use of the DSS, may indicate the relative benefits of the system versus the manual method. If the user feels he can do the same job faster without the system, the credibility of the system will suffer. Although time alone is a dangerous measure (e.g., the DSS may require more time to solve the problem but may give a better answer), time estimation by the user may be matched with other evaluation criteria to provide some type of composite measure of the DSS effectiveness. The method of collecting this estimated completion time should be in the form of a survey presented at the start of the assessment. If the survey is presented at the end of the assessment, the results are based on the user's memory after the fact.

User Knowledge of Problem. An important aspect of the assessment is the knowledge of the compromise beforehand. If the user completely understands the assessment and has organized

this information in his own mind, the assessment will inevitably require less time to complete. If he knows only the basic facts the assessment is likely to take more time. This additional time will come from querying the other data bases in addition to querying outside sources. The user would provide his perception of his familiarity with the problem in response to a survey question. The response would be equated to a number scale from 1 to 10. If the user feels he completely understands the problem, he would mark a "10." This subjective information is no guarantee of the actual knowledge of the user but is still useful.

Last System Use. The user would provide the date in which he last used the system (perhaps this time could be stored in a separate data base). This information will serve two functions. The first function will use the information to determine user acceptability of the system. If it is used regularly, this use may be a sign of user acceptability. Of course, other factors must be taken into account (e.g., number of compromise assessments, who is performing the compromise, etc.). The second function will be keyed to the system. While not currently part of the system, eventually this date could be used by the system to calculate the amount of help the system provides. For example, if the user has not used the system for an extended time period, more information windows on tasks may be provided. Whereas, if the user has recently used the system, no information may be provided except when specifically requested by the user in the form of a "help" function. For this second function, more research will be required to determine the optimal time frames for the

system to make these determinations. An alternative to this previous discussion is to let the user determine the level of help he requires. Under this concept, the system would request the level of help required and then the system would automatically adjust according to this response.

The knowledge of the user about the system will influence the time required to perform an assessment. This subjective assessment provided by the user will be used in conjunction with the information previously discussed. If the user has limited knowledge of the system operation, one would expect the assessment to require a longer completion time and is another factor which can be compared to the estimated manual completion time. The quality of the assessment may also be influenced if the capabilities of the system are not completely understood.

Requirements Knowledge. The knowledge of the requirements of the assessment, as specified in appropriate directives, will influence the quality of the assessment. This lack of knowledge may cause the user to omit important information. The current requirements, as discussed earlier, are vaguely written. The better understanding that a user has, the more likely he is to provide a worthwhile assessment. If useful requirements could be developed by any source, these requirements could be incorporated into the system under some type of "Help" function.

During Assessment. Evaluation of the system under use is perhaps the most difficult aspect of the entire evaluation process. The results of this evaluation is crucial to the success of the sys-

tem, but not to the extent that the quality of the final product suffers. The methods of evaluation during the assessment must be designed to minimize user distractions.

Notepad/Hook Book. The design of the system allows the user to input recommendations for the system and record notes on any subject through the hook book and notepad, respectively. The hook book will provide the most feedback on user satisfaction with the system. In addition, it lays the groundwork for the future evolution of the system. If the hook book entries suggest major changes to the system, these changes may indicate a total dissatisfaction with the system. The entries would have to be individually evaluated to determine the satisfaction or dissatisfaction with the system. The notepad, which is designed only for notes to the user, may include comments about the system operation. If the user enters numerous notes in which he is required to research additional information, these notes may be an indication that the system is not providing the user with enough information. Again, each entry should be evaluated on its own merit.

Voice Recording. The hookbook and notepad are valuable tools; however, the user is required to perform certain actions to access them. These actions may seem distracting to some individuals. To overcome these distractions, a voice recording of the session may aid the evaluation process. A lightweight microphone attached to a voice activated recorder could be attached to the user to monitor hook book and notepad comments. This method would probably provide the least amount of distraction of any evaluation method. The ultimate design of the system would

totally rely on the voice system to perform an assessment and display the results on the computer screen. This system is beyond the scope of this thesis; however it is seen as an ultimate "bound" to pursue.

After Completion of Assessment. The evaluation information obtained prior to and during the assessment coupled with the information obtained after the completion of the assessment will determine user satisfaction with the system. As with the information obtained prior to the assessment, the users' perceptions should be recorded in a survey.

Actual Completion Time. The time required to perform an assessment will aid in determining system usefulness. The completion time may be obtained in a variety of ways. It can done through a log kept by the user or a timer attached to the computer. Other pieces of information to be considered in this comparison are how well the user understood the problem, how well the user understood the requirements, and when the last system use occurred. These additional factors can be used to judge the amount of confidence which can be placed in the actual estimated time. If the time can be considered reliable, the actual completion time should be compared to the logged manual completion time obtained earlier. If time is saved in performing the assessment, the system may be beneficial. If time is saved and the quality of the product goes down, the system is not aiding the decision making process.

Quality of Assessment. The final "assessment" of the system will be partially judged on the quality of the final product

One method to judge the quality of the assessment is to compare the assessment prepared using the DSS with an assessment prepared manually. This comparison could be performed by using another expert (i.e., another individual who did not perform the assessment with computer support) to subjectively determine if the assessment is better than one performed without any support system. This method of evaluation will be extremely labor and time intensive. A study of this method should be performed to determine the relative benefits of the results versus the manpower required to evaluate the system using the comparison method.

User Perceptions. The users' subjective perceptions of the system can also be used to determine the acceptance of the system. The following areas should be measured:

- Rating of ease of use
- Rating of system efficiency
- Subjective rating on the improvement of the assessment
- Confidence in quality of the assessment
- System response time
- Are critical questions answered?
- From the user's standpoint, are the requirements of AFR 205-1 fulfilled?

There are two methods by which user's perceptions may be gathered: 1) written survey, and 2) directly tied to the system itself. When the assessment is completed, the system would automatically display the questions on the screen and await user response.

Long Term. The evaluation of the system over the long term will provide further insight into the users' decision process. As the system evolves, the DSS will become a more powerful tool, not only for the users, but for others outside the organization

The following areas discuss evaluation of the DSS over its lifetime. These areas to be evaluated will not provide any benefits to the system in the foreseeable future.

Pattern Recognition. The ability of the system to recognize a pattern in problem solution would be a powerful tool in compromise assesment. For example, while performing an assessment, the system may recognize the method utilized by the user as having occurred in another assessment. If the system recognized the pattern, the system would be able to either comment on the user's technique or recommend changes to his procedure. A criterion for evaluation is how well the system performs this pattern recognition. As a discipline, pattern recognition is still in its infancy and further discussion is beyond the scope of this research.

Information Sharing. Another long term criterion for evaluation is information sharing. The information in the system may also benefit others who do not use the system on a regular basis, including non-USAF agencies. The system should be designed to easily extract information for use by others. Evaluation in this area will probably be based on the subjective opinions of nonusers.

Strength as Trial Evidence. One of the possible uses of the assessment could be in a court of law (military or civil). This use would occur in cases of espionage or when the classified was lost due to gross negligence. One measure of the system effectiveness would be to determine if the assessment could be used as an aid to convict an individual in a court of law.

Measures for Evaluation. Sprague and Carlson provide a structure for DSS evaluations where the evaluation is conducted as a planned experiment to test one or more hypotheses (18:167). For example, the user responses could be taken and statistically compared using various methods (e.g., the paired t-test or Wilcoxon test). The actual design of the experiment will not be discussed, it is only offered as an approach to evaluate the problem.

Problems With Evaluation. As discussed earlier, establishing criteria is a difficult task. Although the criteria established may provide a statistically sound experiment, the quality of the information used in the experiment may be flawed. This problem may arise anytime that subjective ratings are used to measure attitudes. Four major problems with subjective ratings are:

1. In developing a questionnaire to measure attitudes, one may be trying to quantify that which is not quantifiable and the subsequent analysis may be misleading.
2. Questionnaire respondents may interpret questions differently than intended, and answers to some questions may influence answers to others. Thus unintended impacts may be measured, or a single impact may be interpreted as more than one.
3. Administering questionnaires may be an inconvenience to individuals and expensive (in terms of hours lost by respondents and hours spent by interviewers).
4. The method does not identify the causes of any measured changes. (18:163)

Although most of the discussion in this evaluation section focused on surveys, other methods of evaluation may yield useful results. Whatever the method of evaluation, it should be performed with minimal interference to the routine of the user. Sprague and Carlson believe that a combination of evaluation methods may

result in the best evaluation because of the "variety and complexity of the potential effects (18:167)."

Recommendations

The nature of this research lends itself to many recommendations. Because the system was developed using adaptive design, many specific recommendations were generated from a personal hook book as this thesis was being written. Those recommendations that applied specifically to the system were discussed in Chapter IV. In addition, comments directed at SAC and those concerning DSS, in general, were generated throughout the research.

SAC. These recommendations were generated to aid the continued evolution of the DSS. These requirements are directed at SAC and should be considered before future attempts are made to automate the compromise assessments.

Champion. Since the departure of the previous champion, no new champion has emerged. The champion is an important player in the adaptive design process and without one implementation of the system will be extremely difficult. The champion should be in position of responsibility to provide upper level management support and influence to implement the system. He should be in that position for a reasonable amount of time to provide continuity to the system. This lack of continuity was a contributing factor to the current problem of performing compromise assessments. It is highly recommended that a champion be identified prior to the initiation of any further work in this area.

Priority. A reevaluation by SAC is required to determine the relative priority of the compromise assessment problem to other SAC problems. If it is judged to be a continued area of concern, it is recommended that additional manpower be directed at this task.

Common Procedures. The problem is currently too unstructured. The current procedures are vague and provide no guidance for the final assessment. Following are suggestions to standardize the process.

Working Groups. One recommendation is to initially form a USAF-wide working group and attempt to provide some structure for the problem. For example, this working group could determine the information that is required in the assessment and data that could be used as as aid to the user. This thesis could be used as a "strawman." The goal of the working group should be to determine what is actually needed under AFR 205-1. Once this USAF working group has made their recommendations, a DOD-wide working group should be formed to perform the same function. Structuring the compromise assessment problem will aid in information sharing between DOD components.

Training. It is highly recommended that some type of training program be established for personnel performing assessments. This program can be in the form of management guides, self-inspection checklists, or operating instructions. Because of the high turnover rate in personnel, corporate knowledge is constantly lost. Some means must be developed to retain this lost infomation. Another possibility is to incorporate this system into

computer aided instruction. Because the actual number of compromise assessments is limited, the computer aided instruction function may be used to train the user as the assessment is performed. This function would minimize the time expended in training prior to the assessment.

General DSS Comments. Throughout this thesis effort, comments on DSS in general were noted. Most comments are concerned with the adaptive design process.

Expert. The development of a DSS requires an expert, that is, a user knowledgeable about the task. The development of this DSS was initiated despite the fact that no expert could be found; ultimately, this action was a mistake. Because no expert was available, the author became the expert and made many assumptions which may or may not have been valid. Without an expert, the information modeled probably not a true representation of the system, but it does provide a point of departure.

Main Players. In a project of this magnitude, it is felt that the players should not consist of only two individuals, the user and builder. If an expert cannot be found, one solution is to query as many potential users as possible to determine if the best decision making processes of all of them can be captured. Understandably, the use of too many players will hinder the adaptive design process. A combination of individuals will give a better perspective of the problem and its requirements.

Co-location of Players. The ideal situation would allow the users, builders, and system resources to be co-located. With the players geographically separated, the time to receive feedback

on ideas and changes became a hindrance to this DSS design Given that co-location is not always possible, one suggestion to overcome this separation is a direct computer link between all players. At a predetermined time, all parties can enter the link and exchange ideas via a "conference call." This idea is only one suggestion to overcome the problem of co-location.

Storyboard. The storyboard for this thesis was designed without any technological constraints taken into account. In retrospect, the time and effort required did not seem to provide any additional benefits over designing the system with these constraints in mind. Since the storyboard demanded software capabilities not yet available off-the-shelf, the resulting system and the storyboard were drastically different. If the storyboard relies on current technology, no technological breakthroughs are likely to occur; if it involves technology not yet available, the system will probably not resemble the storyboard. A compromise between the two methods must be reached.

If the storyboard is designed by the user, there should be no impact on the system requirements. Normally, the user understands his requirements beforehand and should integrate these into the storyboard. The storyboard used in this thesis was designed by the author, a surrogate user. Early in the research process, a survey of users was proposed in an attempt to capture the requirements of various users. This survey was discouraged by SAC/SPI and, regretably, never performed. The survey would have greatly improved the final product by getting the user in the feedback loop at the start of the research. This error reinforces

the idea that storyboard should be designed by the user, or, at a minimum, play an active role in the DSS design.

Adaptive Design. The adaptive design process is an excellent concept. Unfortunately, the feedback loop was too time consuming to effectively exercise the process. As discussed earlier, the co-location problem contributed to this time consumption. It is extremely important that "something" be provided to the users to drive the system evolution. If the users do not provide any feedback, they will become disinterested in the final product because of the lack of involvement.

DSS Suitability. After completing this research, it appears that a DSS may not necessarily be suited for completely subjective or completely unstructured problems. While DSS are supposed to be the best alternative to these types of problems, one requirement is never discussed by the authors of DSS articles. All of the DSS described to date, involve an entity which can be quantified. For example, DSS have been used to perform aircrew scheduling functions. Scheduling involves people to be scheduled, planes assigned to people, and a requirement for specific types of personnel on-board, to name a few. All of these factors are quantifiable. Another example of a DSS involves economic forecasting. These types of DSS may involve interest rates, sales quantities, or future costs analysis, which are also quantifiable. The compromise assessment problem may involve a quantifiable entity, but, the impact of the compromise may not be quantifiable. This limiting factor provided the biggest obstacle in

this research. It appears that for a DSS to be successful, all factors involved in the DSS must be, to some extent, quantifiable.

Conclusion

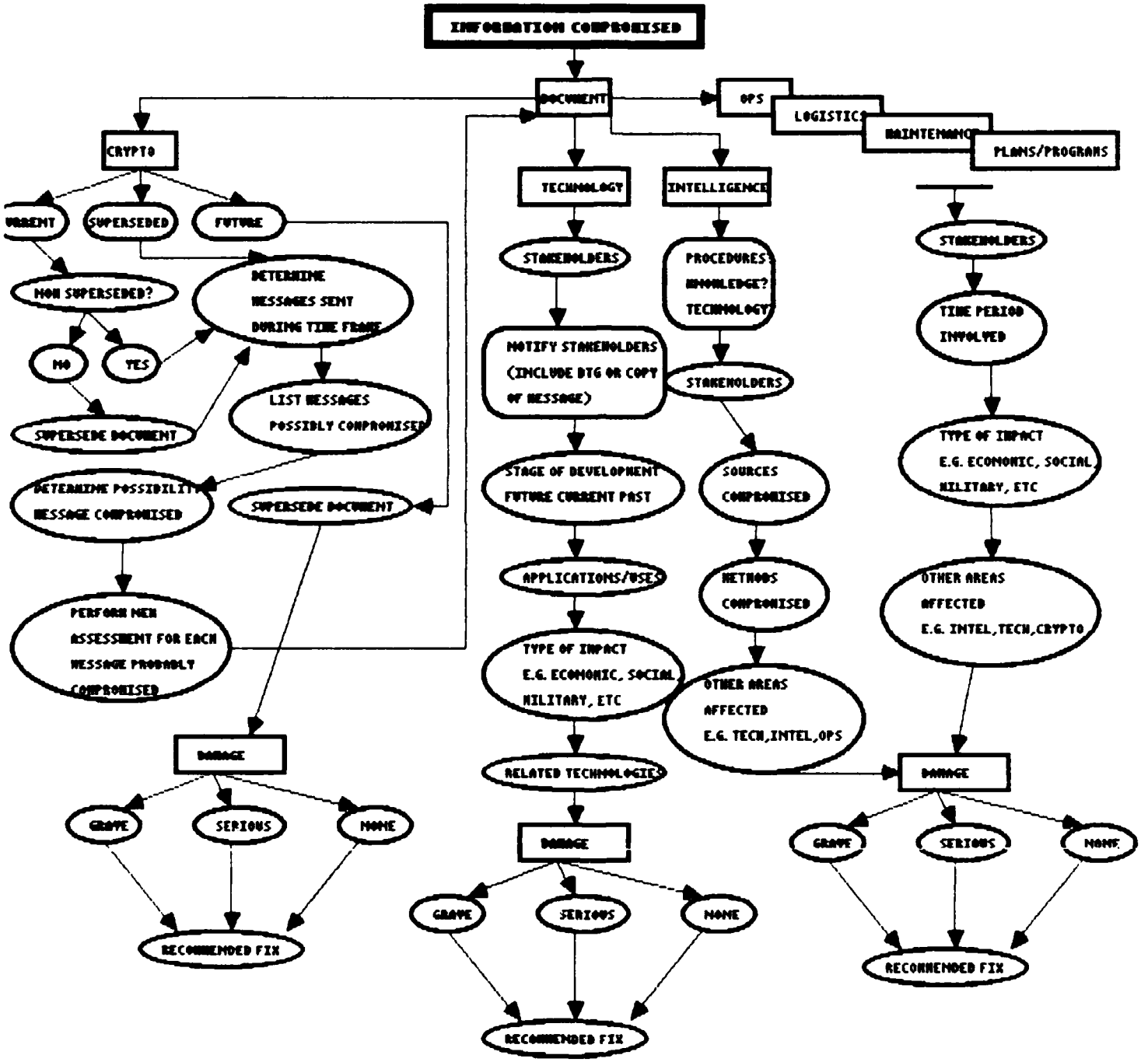
The area of compromise assessment of classified information proved to be an extremely challenging and difficult problem to solve. SAC realized the problem associated with this area and made an attempt to solve it. This thesis was the first known attempt to address the problem. It was never felt that this problem would be completely solved by this effort.

This research was not one which can tout its successes. Much of the time expended in this thesis was spent learning different tools (e.g., solution techniques, software, hardware, etc.) which, at the time, appeared to be beneficial to the research. However, as more about each tool was learned and researched, the less appealing it became as an aid to solve the problem. These failures will be extremely helpful, by serving as lessons learned, in the event others continue research.

The problem of compromised classified information is an extremely important one and cannot be overlooked. SAC should be commended for its recognition of this serious problem. Those USAF elements who foresee no problems with the current system were extremely uncooperative and appeared to be extremely naïve on the severity of the subject. Had those elements been more cooperative, other sources could have been contacted to gather background information on their decision making techniques.

The system presented is not an end product. Hopefully, this thesis can be used as a starting point for further research in this extremely important area.

Appendix A


INFORMATION COMPROMISED
DOCUMENT
OPS
LOGISTICS
MAINTENANCE
PLANS/PROGRAMS
CRYPTO
TECHNOLOGY
INTELLIGENCE
CURRENT
SUPERSEDED
FUTURE
STAKEHOLDERS
PROCEDURES KNOWLEDGE? TECHNOLOGY
STAKEHOLDERS
NOW SUPERSEDED?
DETERMINE MESSAGES SENT DURING TIME FRAME
NO
YES
NOTIFY STAKEHOLDERS (INCLUDE DTG OR COPY OF MESSAGE)
STAKEHOLDERS
TIME PERIOD INVOLVED
LIST MESSAGES POSSIBLY COMPROMISED
SUPERSEDE DOCUMENT
STAGE OF DEVELOPMENT FUTURE CURRENT PAST
SOURCES COMPROMISED
TYPE OF IMPACT E.G. ECONOMIC, SOCIAL MILITARY, ETC
DETERMINE POSSIBILITY MESSAGE COMPROMISED
SUPERSEDE DOCUMENT
APPLICATIONS/USES
METHODS COMPROMISED
OTHER AREAS AFFECTED E.G. INTEL,TECH,CRYPTO
PERFORM MEM ASSESSMENT FOR EACH MESSAGE PROBABLY COMPROMISED
TYPE OF IMPACT E.G. ECONOMIC, SOCIAL MILITARY, ETC
OTHER AREAS AFFECTED E.G. TECH,INTEL,OPS
DAMAGE
RELATED TECHNOLOGIES
DAMAGE
GRAVE
SERIOUS
NONE
GRAVE
SERIOUS
NONE
GRAVE
SERIOUS
NONE
RECOMMENDED FIX
RECOMMENDED FIX
RECOMMENDED FIX

SCREEN: 1
SOURCE: N/A

MAIN DOCUMENT MENU

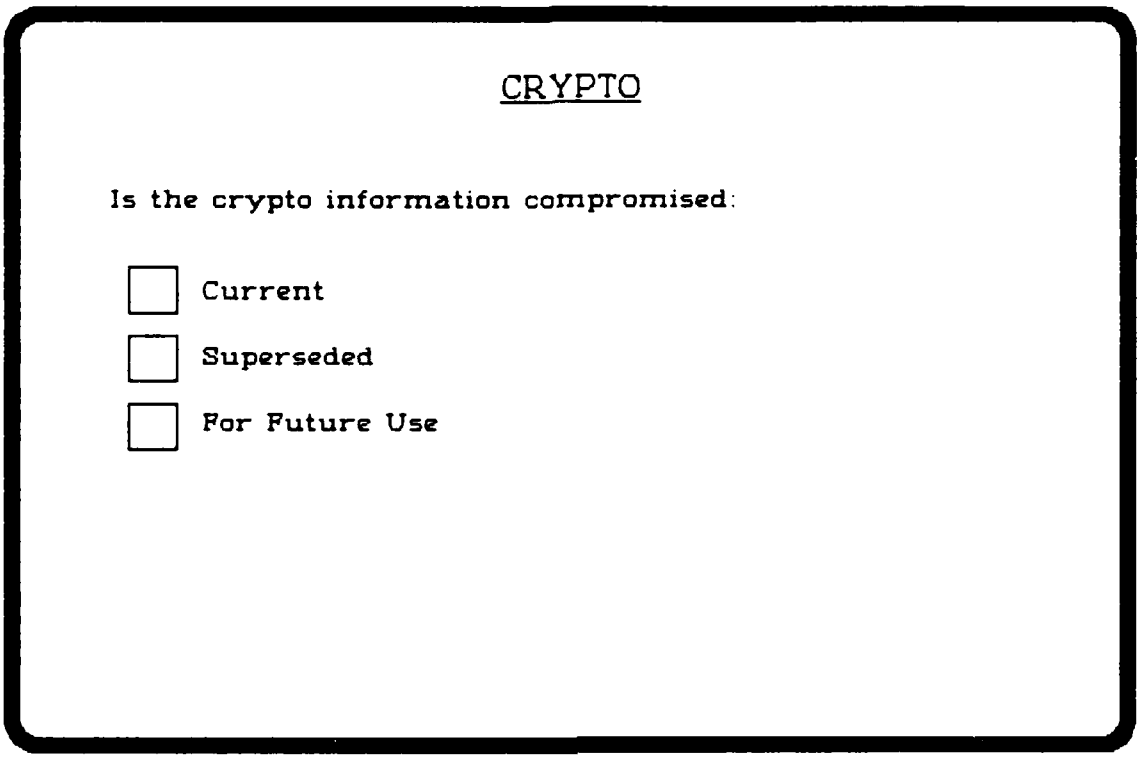
The document compromised what information? (Click pointer in only one box).

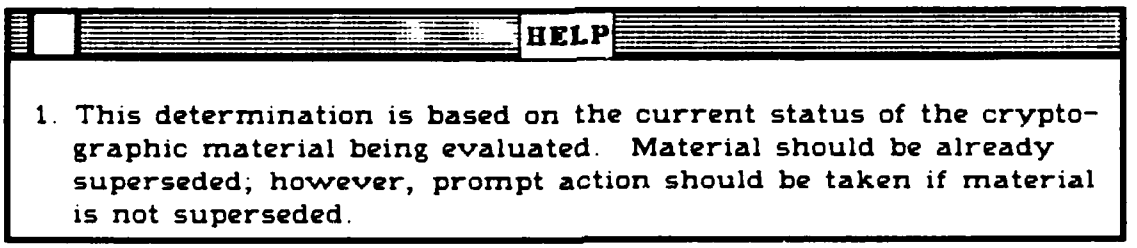
- ☐ Crypto
- ☐ Intelligence
- ☐ Operations
- ☐ Technology
- ☐ Logistics
- ☐ Plans/Programs
- ☐ Maintenance

HELP

1. If the document compromised encompasses more than one box, then work only one area at a time.

SCREEN: 2
SOURCE: 1





ADDITIONAL EXPLANATION: The purpose of this screen is to determine the current status of the documents. If the document has already been used, the possibility exists that all messages sent during the active time period were compromised and need to be evaluated. Basically the same logic applies to the documents currently in use, however, actions should be taken to ensure it is no longer in use. The one that would probably cause the least amount of damage is one to be used in the future since no classified messages should been sent using these crypto documents and should pose no damage to the national security, however, there may be exceptions

SCREEN: 3

SOURCE: 2

CURRENT CRYPTO

Ensure this material is no longer in use. If this material has been superseded, click the pointer in the "Done" box.

☐ Done

☐ Pending

HELP

1. Clicking in the "Pending" box will terminate this session and save the information entered thus far.
2. Clicking in the "Done" box will continue this work session.
3. C heck for electronic methods/encoded messages sent from/ received at the SAC Command Post which may have superseded documents.

SCREEN: 4
SOURCE: 2,3

SUPERSEDED CRYPTO

Determine all messages sent during the time frame that the crypto documents were being used. List these messages as being possibly compromised:

	DTG	ORIGINATOR	TO	SUBJ
1.				
2.				
3.				
4.				
5.				

☐ More messages ☐ Enter

HELP

1. When all messages are entered, click the pointer in the "Enter" box.
2. If more space is needed to enter messages, click in the "More messages" box. The display will allow for more entries continuing at number six.
3. Check for electronic methods/encoded messages sent from/ received at the SAC Command Post which may have superseded documents.

SCREEN: 5
SOURCE: 2

FUTURE CRYPTO

Ensure documents do not become active materials.

☐ Done

☐ Pending

HELP

1. Clicking in the "Pending" box will terminate this session and save the information entered thus far.
2. Clicking in the "Done" will continue this work session.
3. Ensure SAC Command Post notifies all users and maintain a copy of the message transmitted.

SCREEN: 6
SOURCE: 4

MESSAGES COMPROMISED

Determine the possibility that the messages previously listed were actually compromised. List these messages as being probably compromised:

	DTG	ORIGINATOR	TO	SUBJ
1.				
2.				
3.				
4.				
5.				

☐ More messages ☐ Enter

HELP

1. When all messages are entered, click the pointer in the "Enter" box.
2. If more space is needed to enter messages, click in the "More messages" box. The display will allow for more entries continuing at number six.

ADDITIONAL EXPLANATION: The assumption is the message has already been compromised due to the crypto document being compromised. The basic assumption will be a worst case scenario unless other factors are present in which case this would be reflected in the final assessment.

SCREEN: 7

SOURCE: 6

ASSESSMENT OF DAMAGE

A new assessment must be performed on each individual document.

Each new assessment will automatically be cross referenced with this assessment.

Enter additional comments as necessary for this compromise assessment:

☐ More space required ☐ Enter

HELP

1. When all messages are entered, click the pointer in the "Enter" box.
2. If more space is needed to enter comments, click in the "More . . ." box. The display will allow additional space as necessary.

SCREEN: 8
SOURCE: 7,16,22,27

DAMAGE

What is your assessment of the damage done to the U.S. national security as a result of this compromise? (If this compromise is part of a larger compromise assessment, consideration should be given to all other compromises in determining damage.)

☐ Serious

☐ Grave

☐ None

Examples of exceptionally grave damage include armed attacks against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

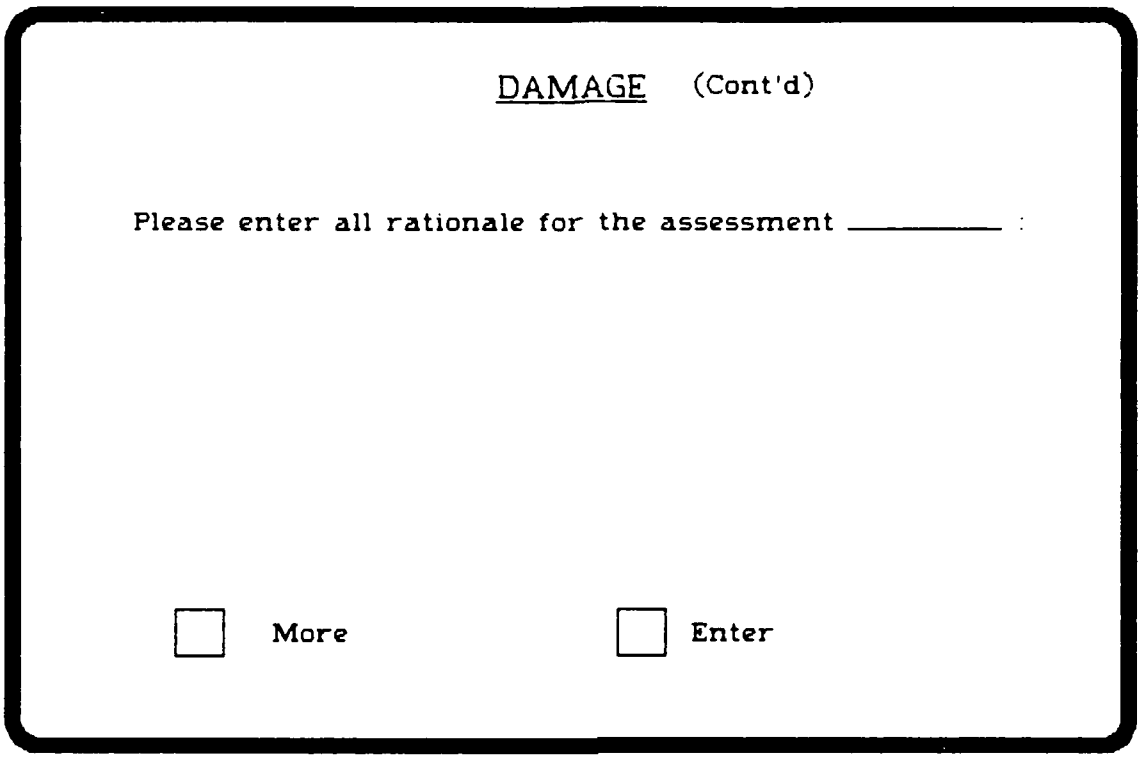
HELP

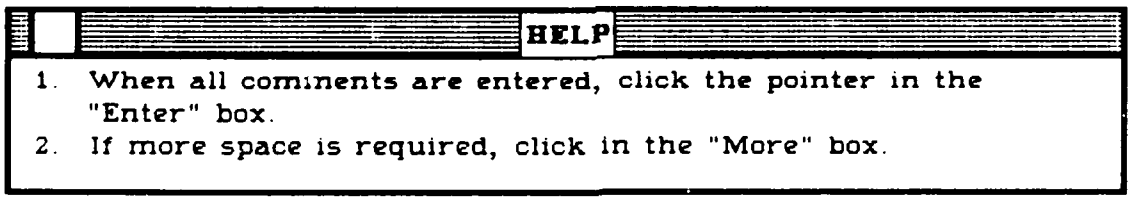
1. SERIOUS:
2. GRAVE:
3. NONE:

Examples of serious damage include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; compromise of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

ADDITIONAL EXPLANATION: This screen and the two following can be thought of as a sort of macro program since all compromises will require an explanation of the damage and fixes required as a result of the compromise.

SCREEN: 9
SOURCE: 8





ADDITIONAL EXPLANATION: If the user has the proper authorization, through the use of a pull down menu, he can scan other assessments for their respective rationales.

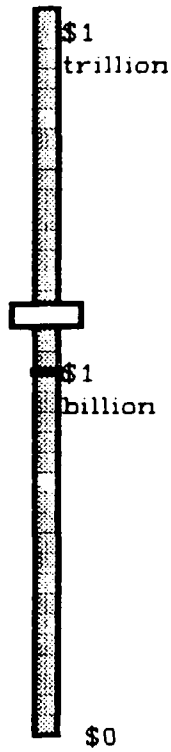
SCREEN: 10

SOURCE: 9

RECOMMENDATIONS

What means will be required to fix the problem caused by the compromise? Can a dollar amount be assigned to the fix? How long will this problem take to be rectified? Other comments.

☐ More ☐ Enter



☐ SET

☐ RESET

HELP

1. When all comments are entered, click the pointer in the "Enter" box.
2. If more space is required, click in the "More" box
3. For entering estimated dollar amount, set the pointer in the in the small rectangular lever and move to the approximation estimation. Click in the set box and a smaller range of values will appear This procedure will continue until an amount to the closest million dollars is determined. If a mistake is made, click in the reset box

SCREEN: 11
SOURCE: 1

TECHNOLOGY

Provide a listing of all stakeholders in this compromise:

	ORG/OFFICE SYMBOL	F (FRIENDLY) OR E(ENEMY)
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		

☐ More ☐ Enter

HELP

1. When all comments are entered, click the pointer in the "Enter" box.
2. If more space is required, click in the "More" box.
3. Place a "F" for friendly or "E" for enemy in the appropriate column.
4. All stakeholders refers to all USAF and DOD components as well as foreign powers.

SCREEN: 12
SOURCE: 11

NOTIFICATION

Provide a listing of the notification of all friendly stakeholders in this compromise:

1.

☐ More ☐ Enter

HELP

1. When all comments are entered for that stakeholder, click the pointer in the "Enter" box.
2. If more space is required, click in the "More" box.
3. "All friendly stakeholders" refers to all USAF and DOD components.

ADDITIONAL EXPLANATION: The information on this screen will be based on the previous screen display and will automatically display those organizations flagged as friendly stakeholders. This purpose of this screen is to allow the user to log/record the actual notification message to stakeholders that the compromise occurred. In most cases, notification will be via electronic message and all units in receipt will have knowledge of all stakeholders. This knowledge may help be helpful to stakeholders in that they will be kept abreast of the compromise assessment process

SCREEN: 13
SOURCE: 12

STATE OF THE ART

What is the current stage of development for the technology contained in the compromised document?

- ☐ Past
- ☐ Current
- ☐ Future

SCREEN: 14
SOURCE: 13

APPLICATIONS

What are the applications and uses for this technology? Be as specific as possible.

☐ More ☐ Enter

HELP

1. When all comments are entered, click the pointer in the "Enter" box.
2. If more space is required, click in the "More" box.

SCREEN: 15
SOURCE: 14

IMPACT

What is the impact of the loss of this compromise? (Examples of possible impact areas include economic, social, and military.) Will the loss impact the enemy's development area? How and when will the enemy use this technology?

☐ More ☐ Enter

HELP

1. When all comments are entered, click the pointer in the "Enter" box.
2. If more space is required, click in the "More" box.

SCREEN: 16
SOURCE: 15

RELATED TECHNOLOGY

List any related technologies which could also have been revealed as a result of this compromise.

1.
2.
3.
4.
5.

☐ More ☐ Enter

HELP

1. When all comments are entered, click the pointer in the "Enter" box.
2. If more space is required, click in the "More" box.

SCREEN: 17
SOURCE: 1

INTELLIGENCE

Did the compromise reveal intelligence:
(Explain in detail)

PROCEDURES: (e.g ELINT, RECCE)

☐ More ☐ Enter

KNOWLEDGE: (e.g. operatives, HUMINT)

☐ More ☐ Enter

TECHNOLOGY: (e.g. Satellite coverages)

☐ More ☐ Enter

☐ **HELP**

1. When all comments are entered, click the pointer in the "Enter" box.
2. If more space is required, click in the "More" box.

SCREEN: 18
SOURCE: 17

INTELLIGENCE STAKEHOLDERS

Provide a listing of all stakeholders in this compromise:

	ORG/OFF SYM	F (FRIENDLY) OR E(ENEMY)
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		

☐ More ☐ Enter

HELP

1. When all comments are entered, click the pointer in the "Enter" box.
2. If more space is required, click in the "More" box.
3. Place a "F" for friendly or "E" for enemy in the appropriate column.
4. All stakeholders refers to all USAF and DOD components as well as foreign powers.

ADDITIONAL EXPLANATION: The stakeholders from different assessments will probably be stored in the same database. In this storyboard, a different screen is used only to show the flow through system.

SCREEN: 19
SOURCE: 18

NOTIFICATION

Provide a listing of the notification of all friendly stakeholders in this compromise:

1.

☐ More ☐ Enter

HELP

1. When all comments are entered for that stakeholder, click the pointer in the "Enter" box.
2. If more space is required, click in the "More" box.
3. "All friendly stakeholders" refers to all USAF and DOD components.

SCREEN: 22
SOURCE: 21

MISCELLANEOUS

Were any other intelligence procedures compromised?

☐ More ☐ Enter

HELP

1. When all comments are entered for that stakeholder, click the pointer in the "Enter" box.
2. If more space is required, click in the "More" box.

SCREEN: 23
SOURCE: 1

OPERATIONS/LOGISTICS/ MAINTENANCE/PLANS/PROGRAMS

Provide a listing of all stakeholders in this compromise:

	ORGANIZATION	F (FRIENDLY) OR E(ENEMY)
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		

☐ More ☐ Enter

HELP

1. When all comments are entered, click the pointer in the "Enter" box.
2. If more space is required, click in the "More" box.
3. Place a "F" for friendly or "E" for enemy in the appropriate column.
4. All stakeholders refers to all USAF and DOD components as well as foreign powers.

SCREEN: 24
SOURCE: 23

NOTIFICATION

Provide a listing of the notification of all friendly stakeholders in this compromise:

1.

☐ More ☐ Enter

HELP

1. When all comments are entered for that stakeholder, click the pointer in the "Enter" box.
2. If more space is required, click in the "More" box.
3. "All friendly stakeholders" refers to all USAF and DOD components.

SCREEN: 25
SOURCE: 24

TIME PERIOD

What is the probable time period that the compromise occurred and what effect did it have on the U.S. national security?

☐ More ☐ Enter

HELP

1. When all comments are entered for that stakeholder, click the pointer in the "Enter" box.
2. If more space is required, click in the "More" box.
3. "All friendly stakeholders" refers to all USAF and DOD components.

IMPACT

What is the impact of the loss of this compromise? (Examples of possible impact areas include economic, social, and military.) Will the loss impact the enemy's development area? How and when will the enemy use this technology?

☐ More ☐ Enter

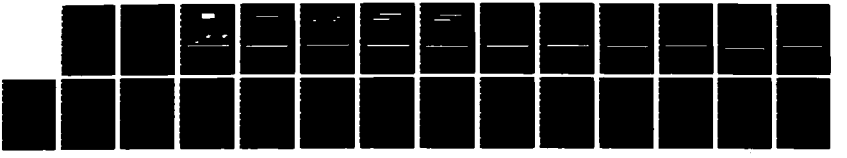
HELP

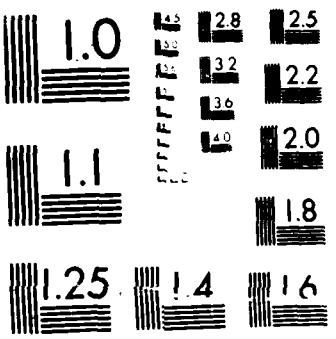
1. When all comments are entered, click the pointer in the "Enter" box.
2. If more space is required, click in the "More" box

AD-A180 232 ADAPTIVE DESIGN OF A DECISION SUPPORT SYSTEM FOR COMPROMISE ASSESSMENT(U) AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH SCHOOL OF ENGI D T SHIRASAGO

2/2

UNCLASSIFIED MAR 87 AFIT/GST/ENS/87M-16 F/G 12/8 NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

SCREEN: 27
SOURCE: 26

MISCELLANEOUS

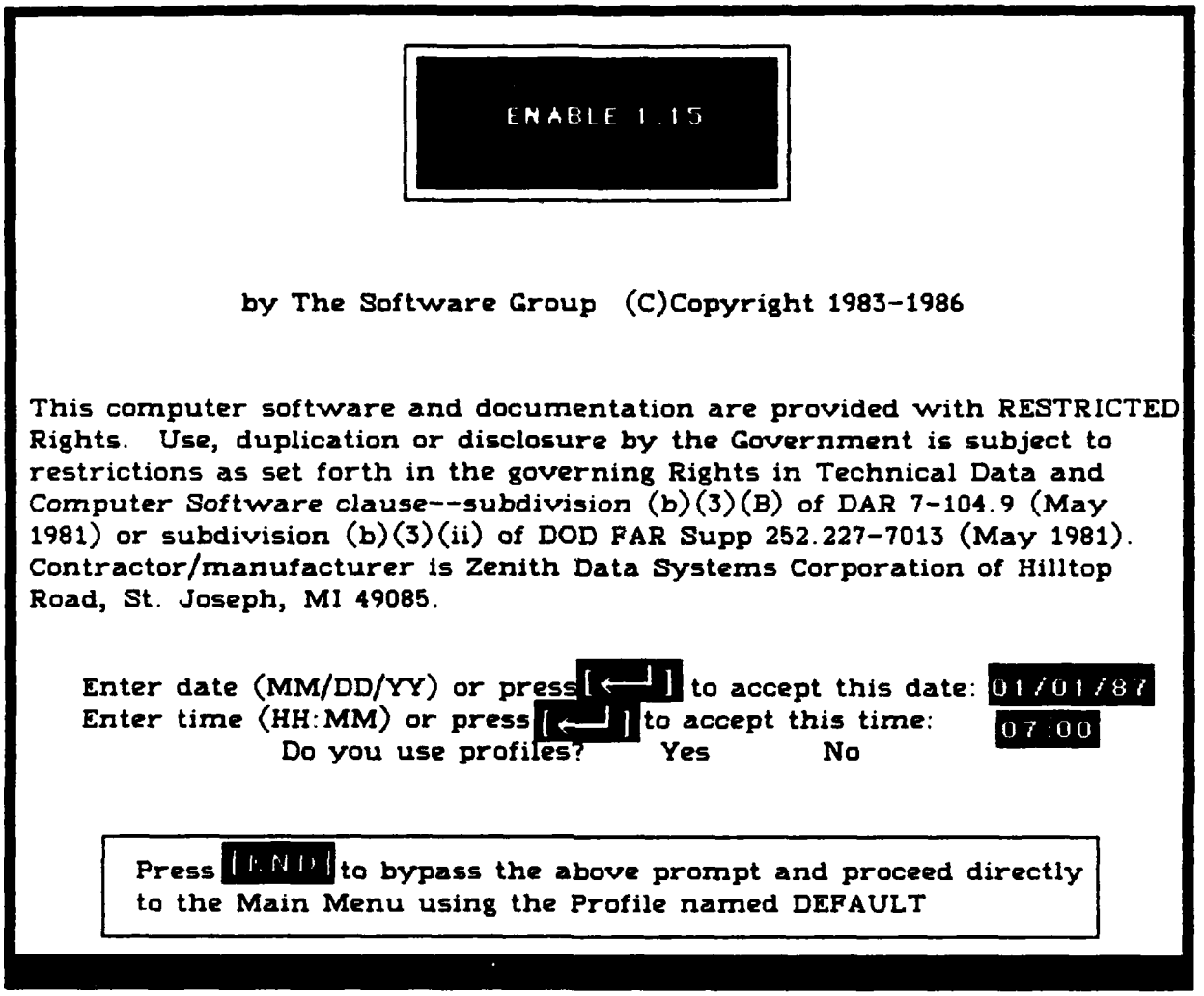
Were any other areas impacted as a result of the compromise? Explain in detail.

☐ More ☐ Enter

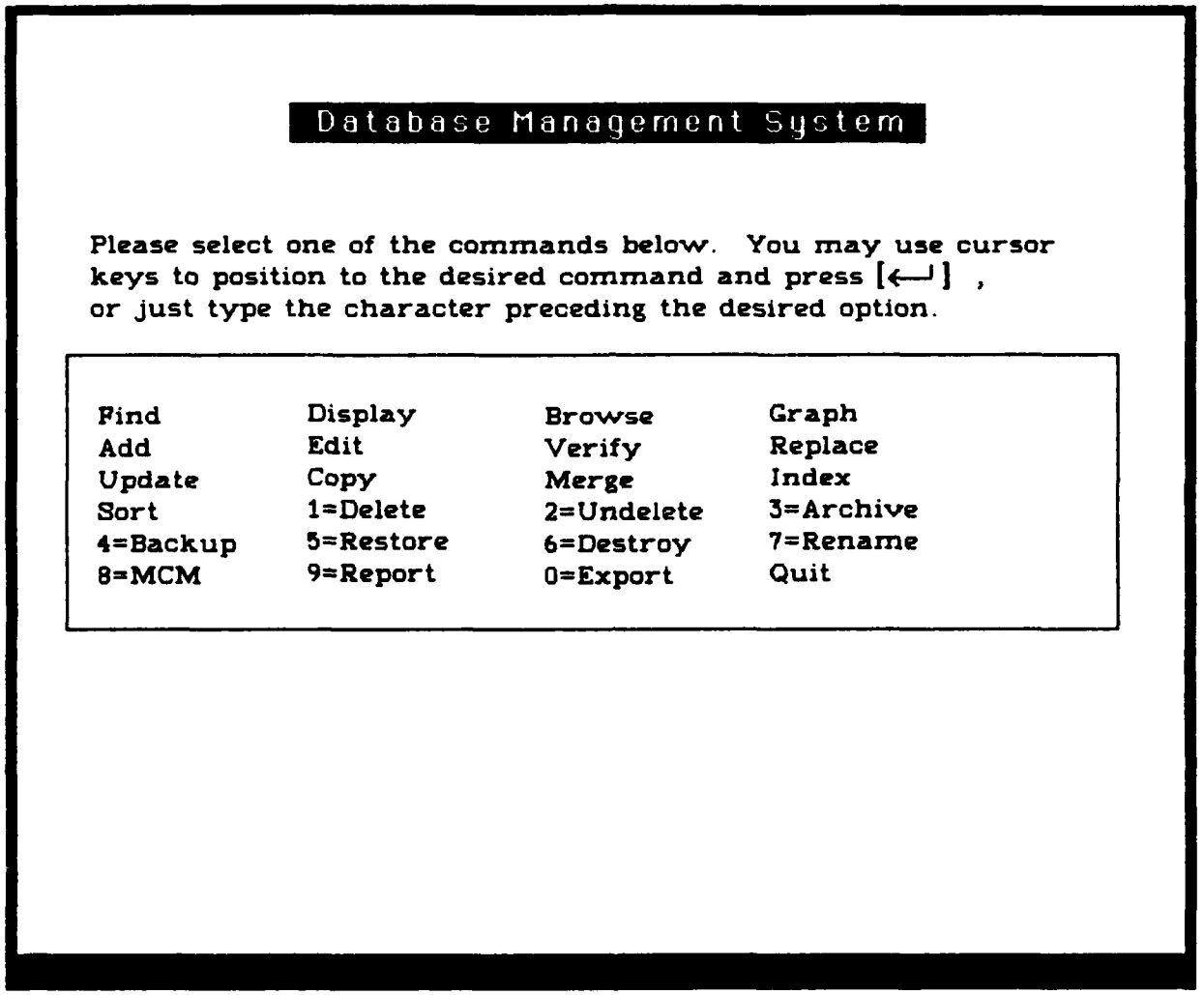
HELP

1. When all comments are entered, click the pointer in the "Enter" box.
2. If more space is required, click in the "More" box.

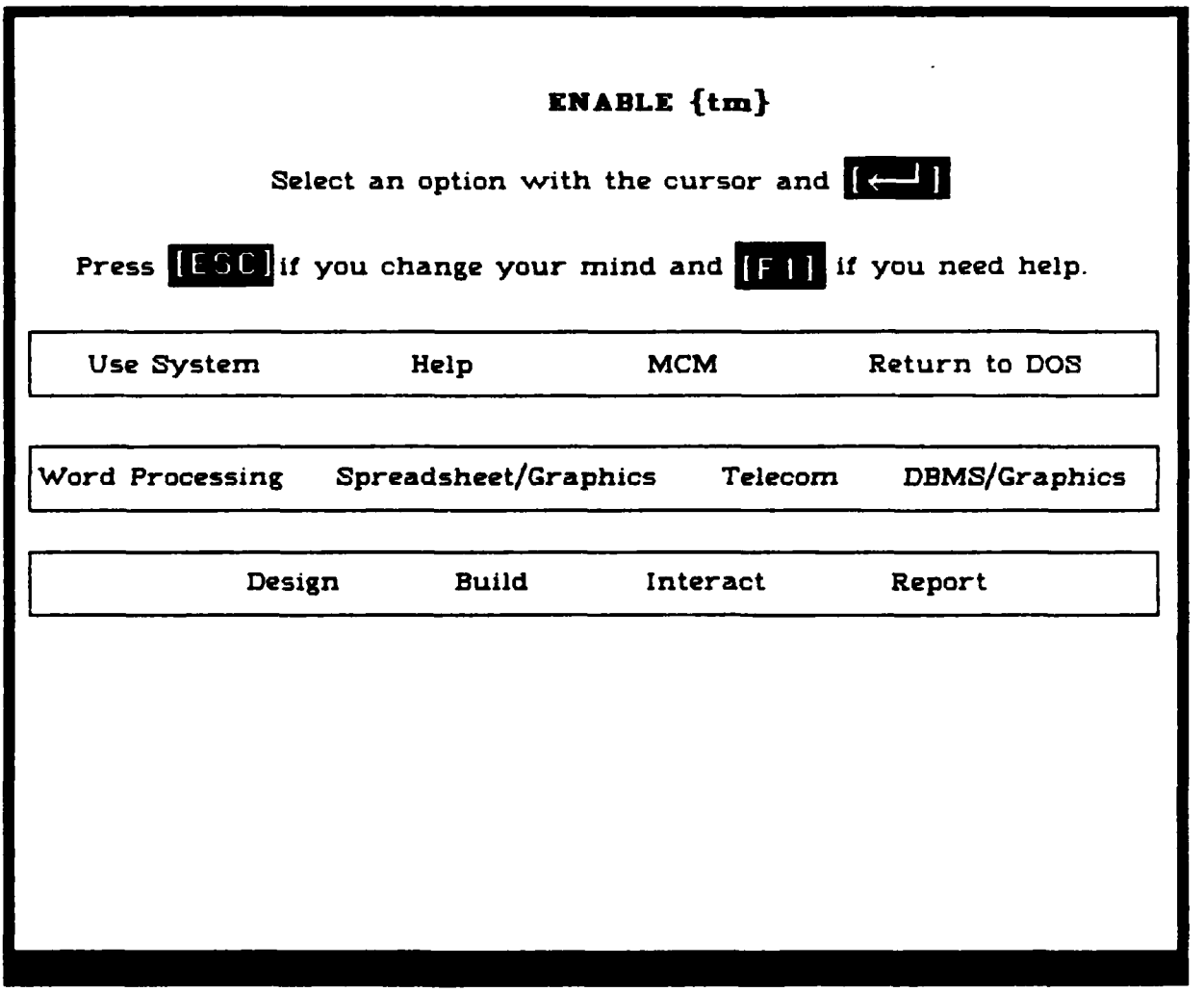
Appendix B



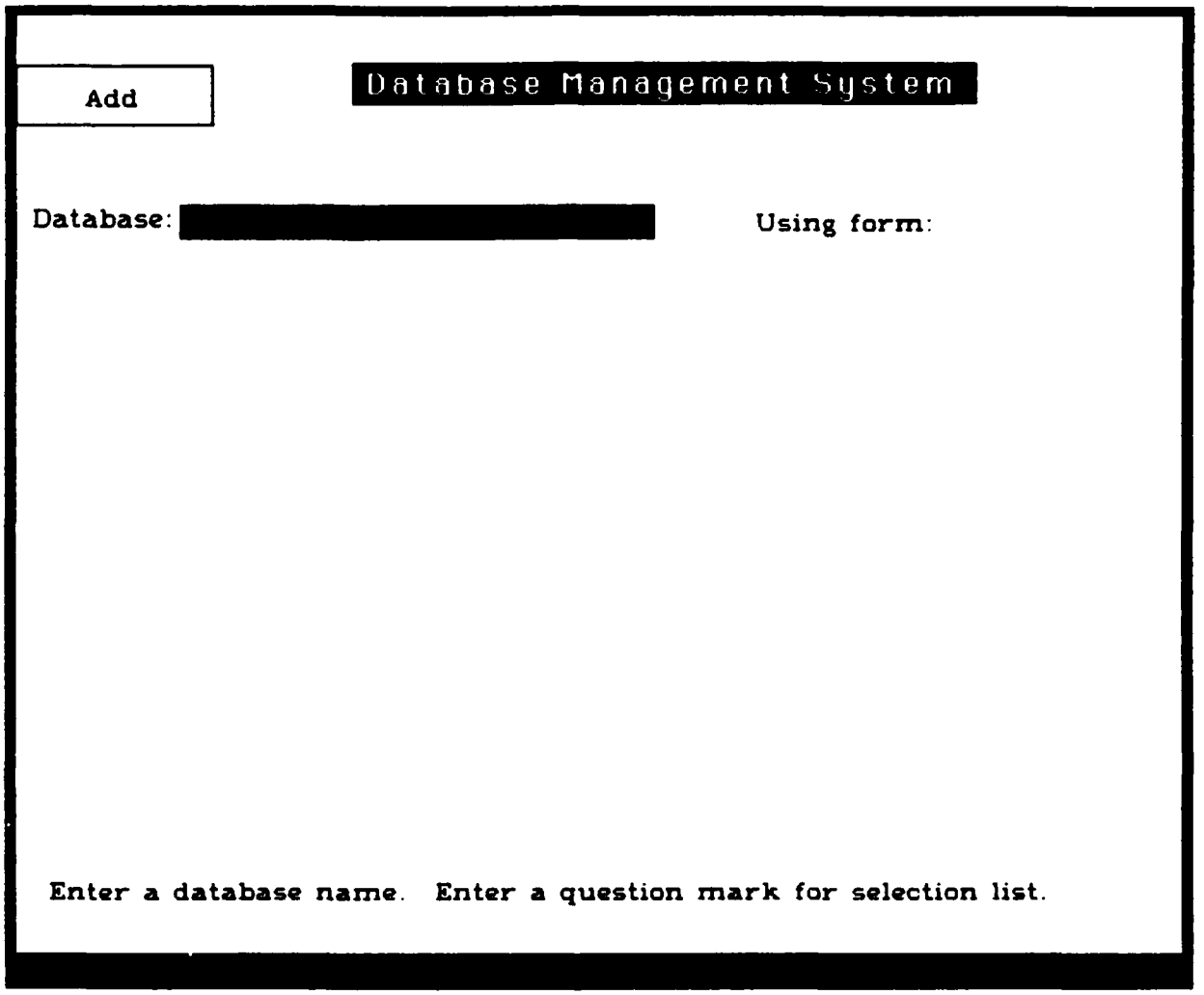
Sign On Screen



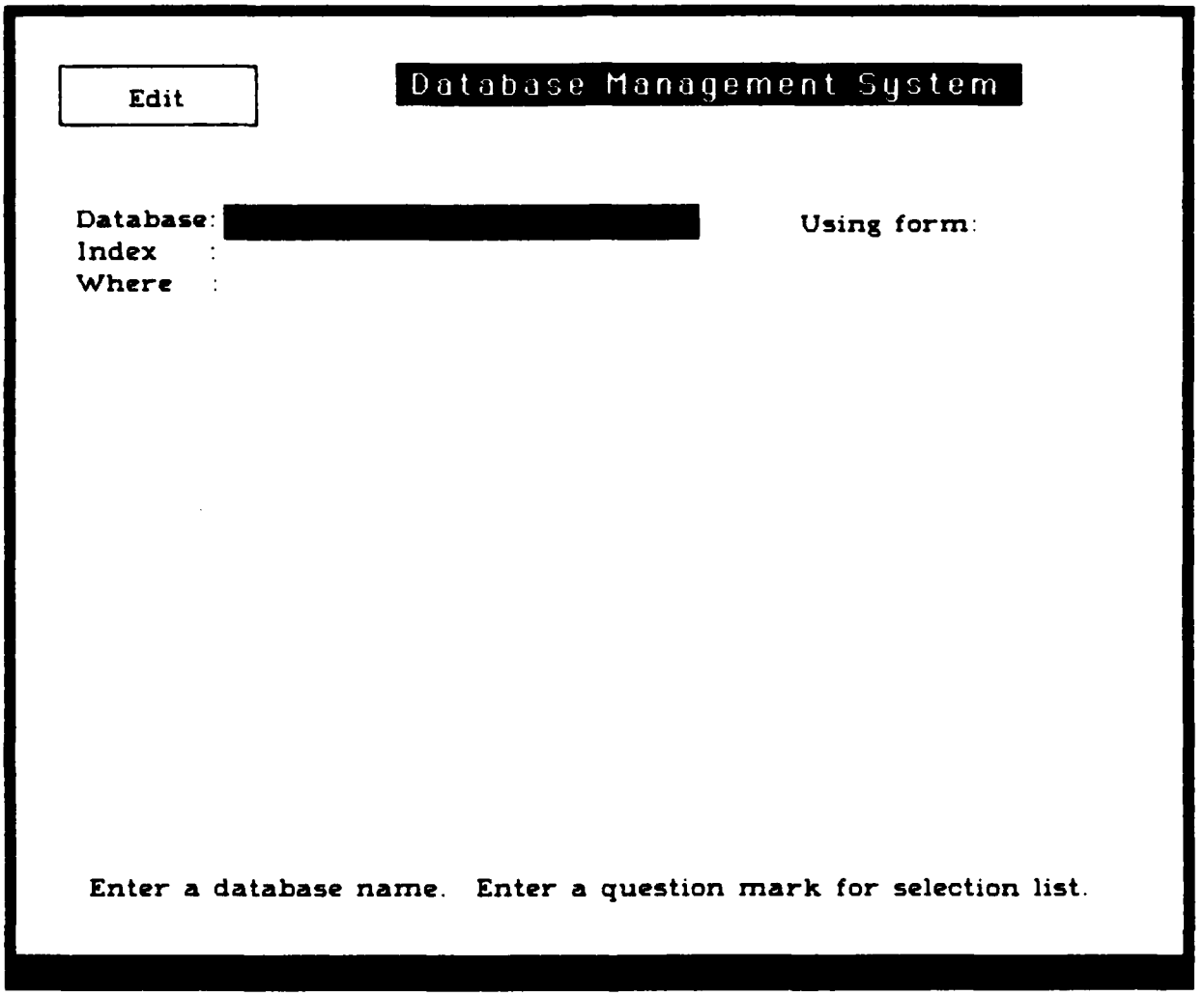
DBMS Command Chart


ENABLE {tm}
Select an option with the cursor and [↵]
Press [ESC] if you change your mind and [F1] if you need help.
Use System
Help
MCM
Return to DOS
Word Processing
Spreadsheet/Graphics
Telecom
DBMS/Graphics
Design
Build
Interact
Report

Main Menu


Add
Database Management System
Database:
Using form:
Enter a database name. Enter a question mark for selection list.

ADD Screen


Edit
Database Management System
Database:
Using form:
Index :
Where :
Enter a database name. Enter a question mark for selection list.

EDIT Screen

DOCUMENT

Compromise Number Assigned:

Document Number:

Date of the document:

Enter the system involved (for multiple entries, press ALT F9 E; when finished press ALT F9 F):

Document Data Base

CRYPTO

Compromise Number Assigned:

Date the crypto material was superseded (this will aid in determining what other material may have been compromised):

List of messages probably compromised (For multiple messages, this process had to be reaccomplished.):

Crypto Data Base

ASSESSMENT

Compromise Number Assigned:

Damage (Specify either "SERIOUS", "GRAVE", or "NONE"):

Description of the compromise:

Assessment of the compromise (include all aspects; if more space is required, continue with another addition to this data base):

Review this assessment on (if no review is required, leaveblank):

Assessment Data Base

OTHER TYPES OF COMPROMISE

Compromise Number Assigned:

Time period that the compromise occurred over:

Assessment (If more space is needed, this process must be reaccomplished.):

"Other Types" Data Base

TECHNOLOGY

Compromise Number Assigned:

Technologies related to the one compromised (For multiple entries, this process will need to be reaccomplished.):

Types of technology compromised (future, current, or past):

Applications for this technology (For multiple entries, this this process will need to be reaccomplished.):

Impact of this loss (any area impacted should be noted and the effects; areas may include economic, social, military, etc.):

Technology Data Base

STAKEHOLDERS

Compromise Number Assigned:

Stakeholder (For multiple stakeholders, this process must be reaccomplished.):

Reason for Stakeholder Inclusion:

Stakeholders Data Base

Appendix C

HOOKBOOK

3/7 - Request from SAC for an expert system
- to help organize the efforts of experts asked to study compromised documents so they are prompted systematically study and report on the materials
- to record the results of their analysis in a retrievable and usable form
- to develop means to assess the cost of a compromised document in real and related costs (maybe using fuzzy set theory)
- wants to use PC/AT standalone system
- user friendly
- document will be stored on laser disks and a keyword indexing system will be available
- should help generate options that will allow experts to systematically categorize the compromised information
- need some capacity to deal with new categories that experts identify
- will forward a copy of an inference engine ESIE

5/8 - Meeting with Maj Valusek and Jackie Henningsen (SAC/NRA)
- want a system to organize the search and leave a trail so the list of all comments can be maintained
- end result is the document categorized
- come up with a utility of what was compromised (cost, value), cost to us, benefits to them
- Bob Weakley at SAC is at SPI

5/27 - Letter from SAC dated 7 May but dated wrong
- might use a data base manager to generate an ID type sheet for users to fill in with full screen display and the cursor automatically jumping to the next line to fill in
- Assessment report used by SAC
  - DAP control number
  - Document number
  - Title
  - Classification
  - Extract
  - Currency/Accuracy
  - Relationship to SAC Weapon Systems
  - Assessment
  - Recommendations

6/18 - Trip to SAC

- Starting to learn what is done currently and what is needed
- My observations as I look at current assessments
  - start with who owns the documents
  - need to keep track of all transactions so other similar tracks can be tracked
  - allow for entry of comments at end of assessment
  - list other assessment numbers that had same attributes or paths through trees (sounds like decision tree type stuff)
  - list agencies involved
  - problem with current system is that material is lost when personnel who performed analysis and did the investigation are gone
  - have the system tell the expert when a review date is coming up if the assessment call for a review
  - who (if known) was info passed to
  - compromised document stored on disk (by optical disk) until recommended period for review is over. Currently saved by SPI and put in storage. [This is a lousy way to handle these assessments]
- I think Mr Weakley agrees that trying to calculate a cost caused by the damage is too much to handle considering nothing has been done at all in the field

9/19 - Start looking at problem solving/decision making in the journals, maybe relational data bases may be applicable.

9/30-10/1 - They use a spreadsheet on paper to list things like:

- ID number e.g. by initials of person who compromised info, followed by a number, and whether it is a document or message
- Originator
- FBI number-if used
- Subject/Title
- Classification
- Cross reference by ID number with other cases
- Comments
- Outgoing messages - usually to request assistance in compromise assessment

-Reply/Review/Results

- They assign dollar costs to a compromise based on the cost to fix the damage caused by the compromise→sounds like this is extremely vague
- If a problem involves other services, the Navy has focal points to pass them on to→talking to the USAF focal point was disillusioning, no wonder there's problems

10/9 - Research objective→initiate a DSS to aid SAC in assessing damage caused by the compromise of classified information
- System should combine decision trees and word processing. This would allow the user to progress through a tree structure while at the same time documenting the decision process that he went through to come up with the assessment. This documentation would be useful in future reviews because all elements of the decision process would be available. The system should log all transactions made and provide the user with a printout at his request. I would also like to see a "mouse" input device be used to aid the user, rather than the user having to learn commands to drive the computer

10/10 - Generate a massive tree diagram depicting the major areas which could probably be compromised: technology, document, and person. This can be thought of as a flow chart to handle the different scenarios. This in itself is going to extremely hard to handle.

10/17- Looks like the problem is too big to handle so the decision was made to limit the scope of the problem to only documents and a new chart depicting only this area must be developed

10/29 - Meeting with Lt Col Valusek
- Start coming up with a system
- Log how things evolved especially for the kernel
- Start setting up storyboard to just the top level and then into document level
- Data base management
- Input reports by keyword to "search" and provide ways to do it
- Provide a Help command that gives suggestions to aid the user
- Hit a key to go elsewhere to find the info
- Start thinking of relations for data base design
- Notepad → I think like the Mac's way of handling this function
  - combine the notepad and suspence file into one

- maintain a running sequence of notes
- free flowing
- possible store date and time automatically on the notepad

- Want the system to work more than one area when performing an assessment

- Start talking to others about the software program Enable to see how it handles word processing

11/25 - Starting to consider some evaluation criteria. I think it is important to recieve comment prior to, during, and after, the session to determine how the system performed. Also the long term use should also be considered. These are some the things that should be considered:

PRIOR

Estimated time to completion manually
Understand the problem completely?
Last time the system was used
Understand the system
Understand the requirements

DURING

Through the use of the notepad, comments can be retrieved to determine user satisfaction/complaints/ comments
Possibly hook a lightweight microphone to the user to record the user's feelings on the system while in use, this would cut down on the break in continuity by having to call up the notepad

AFTER

Actual time to completion
Turing test w/ another qualified individual (if possible)
Understand the problem better than at the start
Extent of use
Ease of use
Efficiency
Solution improvement
Confidence in solution
Response time
Critical questions answered
Understand the system
Requirements from AFR 205-1 satisfied

LONG TERM

Ability to detect pattern recognition
Does it facilitate information sharing?

Could it help convict somebody

12/9 - Macros are being designed to allow the user to perform actions as data entry with a few keystrokes as opposed to many.

- Consider some type of field linking to overcome the 254 character limit
- Maybe use a macro to leave one form then go to another then at the end write all of this into one database

12/11 - Now considering having multiple forms all reading into one data base and allowing the user to choose which entries he will make. Using one data base should allow the user to have an easier time accessing the data base and finding any possible related areas which will aid in the assessment. Should be faster.

12/13 - Having trouble trying to accomodate multiple entries for a specific field. Maybe there is a way to enter in all values in one field and when there is a query, just let the system scan the entire field for a certain stakeholder.

- Received a reply received 12-11-86) from SAC on the initial storyboard. Comments on the flow chart are as follows:

  1) Since the damage assessment block is the same at end of all streams, it could be written once at the bottom of the flow chart

  2) Terms may need [to be] spelled out more carefully on help screens--what do you mean by "document"? Are messages from crypto included?

  3) I can see difficulty in fitting all that is needed on one page for the flow chart, but I'm uncomfortable with the implied relationships of the arrows coming out of [the] document. What is the level of importance of intelligence, technology and say logistics? Are they the same as Crypto?

  4) I would avoid screen choices that end the session until further action is accomplished since the experts brought in for [the] assessment will frequently have a limited block of time to work on this. Find an option where they can proceed, but an outside tasking for SPI or other staff is noted.

  5) You have shown a large view, but I'd like to see you take one category and break it down more thoroughly if possible. Even if the others are merely sketched, this would help. For instance with

technology, I would try to ask more information with common category multiple choice information before you asked the assessor to start writing paragraphs. This was one downfalling of the present system.

6) The storyboard entries won't change much, but I'm inclined to feel the flow chart should look more like this: (see next page).

7) Screen 8: Needs more categories; also need a "heading" category.

8) Screen 10: Add: "Estimate $ amount if possible ____". A little too gimmickly. For $ amount consider just writing a tasking again or just have them enter it.

9) Screen 11: Define stakeholders;does it include incidental interest? Maybe rank order.

10) Screen 12: Good. Task list. Generate/store the message.

11) Screen 13: Spell thes out better. In operation R+D, OT+E,etc. Be sure you have a way of handling multiple technologies as a given document may combine more than one. This capability may have to "back reach" to earlier pages.

12) Screen 15: Put these into multiple choices then have them comment

13) Screen 16: Good.

14) Screen 17: How does this relate to previous screen on technology. When would one be used and not other.

15) Screen 26: Povide more choices.

- Probably should have one more than one data base and relations based on what is entered in the main data base.

12/15 - Possible way of handling the multiple entries: maybe have one big field for stakeholders and use some type of search function to see if a certain stakeholder is present.

1/5 - Need to consider the hookbook and notepad as a separate data base. Will probably put this on a menu choice.

1/10 - Would be extremely beneficial to have multiple windows open when entering data into a specific data base, but this doesn't work since the data base function needs to use a full window. Z-248 now being used.

- The window size of the notepad/hookbook need to be changed/reduced to keep working screen displayed to user.
- A macro will get in and out of the notepad/hookbook.
- Write macros for:
  auto log on

notepad
hookbook
document
assessment
stakeholders
crypto
technology
others
mostly used to get into other data bases based on relations

1/11 - Need to add a function to "add" documents to the data base and get you back to where you were working without having to make the user enter anything.
- Multiple screens will not work so this is a obstacle. For follow on research, maybe a spreadsheet will work better.
- Maybe use a special block to key the system that the user is not finished so if a user goes to another data base, he can return to a previous activity.

1/12 - Might be nice to have a tree diagram to show where you are at in the system. Maybe give the user a warm fuzzy where the system is taking him.
- Still need to find a way to get the user back to where he was working before. Maybe use the SYS:RECORD lined up in descending order so that the last one entered is automatically recalled. So use a macro to sort then edit the last record entered.
- Sort and edit will not work like imagined above.

1/14 - Need a way to keep the compromise number in memory so the system knows to get back to the one that the user was working on (if he goes to a notepad/hookbook). The reason for this is that the system can get back to the last database but not to the same or last record entered. The compromise number is also needed in case an entry may be made and the next entry should not force the user to enter the number again.
- To go with above, need to have a macro that can at least get back to previous activity.
- Have a way to save the compromise number:
  {%compnumb} in a macro will save it in the MCM
- Need to have two different menus: one for adding in stuff and the other for querying databases.
- Need to have a help function for first/new users

- Way down in the future, need to have a system that protects certain records. May have a case where an individual does not have access to a certain set of records.
- Change the information in the menu function to a help function once users know how to use the system.

BIBLIOGRAPHY

1. Bishop, Katherine. "Navy Radioman Guilty of Spying for the Russians," New York Times, 134:I,5 (25 July 1986).

2. Brinkley, Joel. "Experts Tell of Spying Surge and Vulnerable U.S. Secrets," New York Times, 134:I,2 (2 June 1985).

3 Conrad, Richard D. Personal interview. AFLC/SPI, Wright-Patterson AFB, OH, 2 October 1986.

4. Department of the Air Force. Information Security Program Regulation. AFR 205-1. Washington: HQ USAF, 7 December 1982.

5. Department of the Air Force. Environmental Impact Analysis Process (EIAP). AFR 19-2. Washington: HQ USAF, 19 August 1982.

6. Feinstein, J.L. and Frederick Siems. "EDAAS: An Expert System at the US Environmental Protection Agency for Avoiding Disclosure of Confidential Business Information," Expert Systems, 2:72-85 (April 1985).

7. Ford, F. Nelson. "Decision Support Systems and Expert Systems: A Comparison," Information & Management, 8:21-26 (January 1985).

8. Henningsen, Jacqueline. Personal Correspondence. HQ SAC/NRA, Offutt AFB, NE, 7 March 1986.

9. Henningsen, Jacqueline. Personal Correspondence. HQ SAC/NRA, Offutt AFB, NE, December 1986.

10. Hetman, François. Society and the Assessment of Technology. Paris: Organisation for Economic Co-operation and Development, 1973.

11. Keen, Peter G.W. "Adaptive Design For Decision Support Systems," Data Base, 12:15-25 (Fall 1980).

12. Lemonn, Albert. Telephone interview. HQ AFOSP/SPI, Kirtland AFB, NM, 23 July 1986.

13. "Pentagon Making Major Effort to Plug Security Leaks." Program Manager, XIV:17 (November-December 1985).

14. Scott, John J., Jr. Chief, Information Security Branch, Aeronautical Systems Division. Personal interview. ASD/SPI, Wright-Patterson AFB, OH, 2 October 1986.

15. Schnell, Kenneth F. Assistant Professor of Engineering Management. Personal interview. School of Civil Engineering, Air Force Institute of Technology (AU), Wright Patterson AFB, OH, 8 September 1986.

16. Shenon, Philip. "A 4th Spy Suspect With Ties to Navy is Seized on Coast," New York Times, 134:I,1 (4 June 1985).

17. Spencer, Daniel Lloyd. Technology Gap in Perspective. New York: Spartan Books, 1970.

18. Sprague, Ralph H. and Eric D. Carlson. Building Effective Decision Support Systems. Englewood Cliffs: Prentice-Hall, Inc., 1982.

19. Turban, Efraim and Paul R. Watkins. "Integrating Expert Systems and Decision Support Systems," Decision Support Systems: Putting Theory Into Practice, edited by Ralph H. Sprague, Jr. and Hugh J. Watson. Englewood Cliffs: Prentice-Hall, Inc., 1986.

20. Valenti, Ben. Damage Assessment Task Force Member. Personal interview. Naval Security and Investigative Command, Director of Naval Intelligence, Washington, D.C., 30 September 1986.

21. Valusek, John R. Lecture materials distributed in OPER 652, Decision Support Systems. School of Engineering, Air Force Institute of Technology (AU), Wright-Patterson AFB, OH, October 1986.

VITA

Captain Dale T. Shirasago was born 7 September 1958 in Los Angeles, California. He graduated from the United States Air Force Academy from which he received the degree of Bachelor of Science in International Affairs in May 1980. Upon graduation, he became a Titan II missile launch officer for the 381 Strategic Missile Wing at McConnell AFB, Kansas, serving as a deputy crew commander instructor and crew commander. In 1983, he was selected to participate in the USAF Project Ready Merlin, the first ever integrated flight training program for the Ground Launched Cruise Missile, at Davis-Monthan AFB, Arizona. In 1984, his unit was deployed to open a new USAF base, Comiso AS, Italy. He served as the senior evaluator and instructor for both deputy crew commanders and crew commanders at the 487th Tactical Missile Wing, until entering the School of Engineering, Air Force Institute of Technology, in August 1985.

Permanent Address: 2951-5th Avenue
Los Angeles, California 90018

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1a. REPORT SECURITY CLASSIFICATION: UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT: Approved for public release; distribution unlimited.
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S): AFIT/GST/ENS/87M-16	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION: School of Engineering; 6b. OFFICE SYMBOL (If applicable): AFIT/ENS	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State, and ZIP Code): Air Force Institute of Technology, Wright-Patterson AFB, Ohio 45433	7b. ADDRESS (City, State, and ZIP Code)
8a. NAME OF FUNDING/SPONSORING ORGANIZATION; 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code)	10. SOURCE OF FUNDING NUMBERS: PROGRAM ELEMENT NO; PROJECT NO; TASK NO; WORK UNIT ACCESSION NO

11. TITLE (Include Security Classification)
ADAPTIVE DESIGN OF A DECISION SUPPORT SYSTEM FOR COMPROMISE ASSESSMENT

12. PERSONAL AUTHOR(S)
Dale T. Shirasago, B.S., Capt, USAF

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
MS Thesis	FROM _____ TO _____	1987 March	116

16. SUPPLEMENTARY NOTATION

Approved for public release IAW AFR 190-1.
LYNN E. WOLAVER 5 May 87
Dean for Research and Professional Development
Air Force Institute of Technology (AU)
Wright-Patterson AFB OH 45433

17. COSATI CODES		
FIELD	GROUP	SUB-GROUP
05	02	

18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
Adaptive Design, Decision Support Systems, Classified Material Compromise

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

This project researched the adaptive design process and attempted to provide an aid to users who perform assessments of compromised classified information. The background research of this subject did not indicate any previous attempts in solving this problem. Because of this absence of information, the lack of specific guidelines for compromise assessments, and inadequate bookkeeping of information, the scope of the problem was reduced to classified information contained only in documents. The document area appeared to have the most structure and the highest probability of success.

The adaptive design process started after current operating procedures were reviewed. A storyboard (graphic representations of the system unconstrained by current technology) was depicted and used as a goal for the final system. The storyboard was designed to be "user friendly." Since no off-the-shelf software could be found to implement the storyboard, a redesign of the system was performed.

The "first cut" system used an integrated software package as its foundation. This
(continued on reverse)

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL: John R. Valusek, Lt Colonel, USAF	22b. TELEPHONE (Include Area Code): 513-255-3362; 22c. OFFICE SYMBOL: AFIT/ENS

DD Form 1473, JUN 86 *Previous editions are obsolete.*

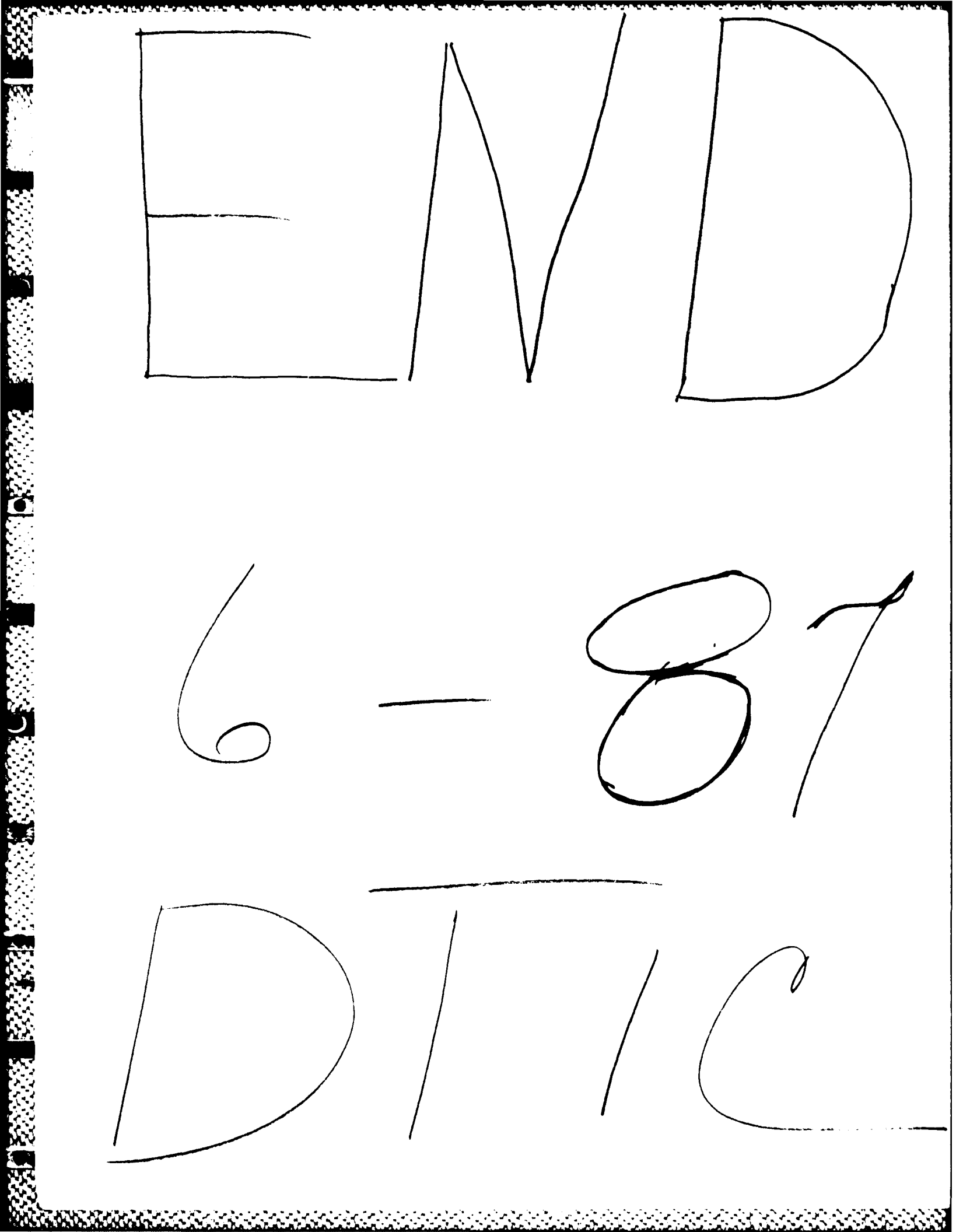
SECURITY CLASSIFICATION OF THIS PAGE

UNCLASSIFIED

Block 19 (Continued)
system relied on a variety of data bases to maintain information pertaining to classified documents. Function menus were used to access other data bases. The system also allows for the entry of suggested improvements, maintained in the "hook book," and provides a notepad function for user convenience.

The system presented is not a final product and should evlove as the problem becomes more defined. The results of this study indicate that further research be conducted utilizing more resources and manpower.

Thesis Chairman: John R. Valusek, Lt Colonel, USAF
Associate Professor of Operations Research


END
6-87
DTIC